DISEÑO Y PLANIFICACIÓN DEL SUB-SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE BACKUPS BASADA EN LA NORMA ISO/IEC 27000 EN LA EMPRESA DE TRANSPORTE ESPECIAL DE PASAJEROS TESCOTUR LTDA.

LÍNEA TEMÁTICA: GESTIÓN DEL RIESGO

DENNYS VIVIANA FARFÁN PÁEZ
ROBERT NICOLÁS MURILLO DÍAZ

JUAN CARLOS ALARCÓN SUESCÚN
ASESOR

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA COHORTE 28
BOGOTÁ D.C.
2016

DISEÑO Y PLANIFICACIÓN DEL SUB-SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE BACKUPS BASADA EN LA NORMA ISO/IEC 27000 EN LA EMPRESA DE TRANSPORTE ESPECIAL DE PASAJEROS TESCOTUR LTDA.

LÍNEA TEMÁTICA: GESTIÓN DEL RIESGO

DENNYS VIVIANA FARFÁN PÁEZ
ROBERT NICOLÁS MURILLO DÍAZ

Proyecto de grado para optar al título de
Especialista en Seguridad Informática

JUAN CARLOS ALARCÓN SUESCÚN
ASESOR

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA COHORTE 28
BOGOTÁ D.C.
2016

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C. 7 de febrero de 2017

Dedicamos este trabajo a nuestras familias, quienes nos han apoyado en nuestro proceso formativo, entendiendo la dedicación de tiempo que necesitamos para alcanzar esta meta.

También a la Universidad Piloto de Colombia, especialmente a los docentes, por compartir con nosotros sus conocimientos y experiencias, pensando siempre en formar profesionales íntegros; y a nuestros compañeros del grupo ESI28 porque aun finalizando las materias, continuaron apoyándonos durante la ejecución de este proyecto.

Viviana, Nicolás

AGRADECIMIENTOS

Queremos agradecer primeramente a Dios, a nuestras familias quienes a lo largo de este camino de formación académica han estado apoyándonos, especialmente a nuestros padres. También agradecemos al Ingeniero Juan Carlos Alarcón Suescún por la orientación brindada y sus aportes de experiencia profesional en nuestro proyecto, finalmente a Tescotur Ltda., por darnos la confianza de entrar a su organización para la elaboración de este proyecto de grado.

CONTENIDO

pág.

INTRODUCCIÓN **15**
1. JUSTIFICACIÓN **16**
2. DEFINICIÓN DEL PROBLEMA **17**
2.1 FORMULACIÓN DEL PROBLEMA 17
2.2 OBJETIVOS 17
2.2.1 Objetivo general 17
2.2.2 Objetivos específicos. 17
2.3 TIPO DE INVESTIGACIÓN 18
2.4 HIPÓTESIS 18
2.4.1 Hipótesis investigativa (Hi) 18
2.4.2 Hipótesis nula (Ho) 18
2.5 VARIABLES 18
2.5.1 Variables dependientes. 18
2.5.2 Variables independientes. 19
3. MARCO TEÓRICO **20**
3.1 CONCEPTOS GENERALES 20
4. METODOLOGÍA **24**
5. DESARROLLO DEL PROYECTO **26**
5.1 ESTABLECIMIENTO DEL CONTEXTO 26
5.1.1 Consideraciones generales 26
5.1.2 Criterios básicos 26
5.1.2.1 Criterio de evaluación del riesgo 26
5.1.2.2 Criterios de probabilidad 27
5.1.2.3 Criterios de impacto 28
5.1.2.4 Criterios de aceptación del riesgo 28
5.2 VALORACIÓN DEL RIESGO 29
5.2.1 Identificación de los Activos 29

5.2.2 Identificación de las amenazas 30
5.2.3 Identificación de las vulnerabilidades 30
5.2.4 Identificación de las consecuencias 34
5.3 ESTIMACIÓN DEL RIESGO 35
5.3.1 Metodología para la estimación del riesgo 35
5.3.2 Evaluación de las consecuencias 35
6. TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN .38
6.1 DESCRIPCIÓN GENERAL DEL TRATAMIENTO DEL RIESGO 38
6.2 REDUCCIÓN DEL RIESGO 40
7. DECLARACIÓN DE APLICABILIDAD 48
7.1 EVALUACIÓN DE CUMPLIMIENTO 49
7.2 RESULTADOS DE LA EVALUACIÓN DE CUMPLIMIENTO 57
8. PLAN DE TRATAMIENTO DE RIESGOS 59
8.1 COSTO – BENEFICIO CONTROLES SELECCIONADOS 59
8.2 PLAN DE TRATAMIENTO DE RIESGOS Y GUÍA DE IMPLANTACIÓN DE CONTROLES 60
9. OBJETIVOS DE SEGURIDAD DE INFORMACIÓN 68
10. PLAN DE TOMA DE CONCIENCIA 81
11. PLAN DE COMUNICACIONES 83
12. CONCLUSIONES 85
13. RECOMENDACIONES 87
ANEXOS 89

LISTA DE CUADROS

pág.

Cuadro 1. Variables dependientes 19
Cuadro 2. Variables independientes 19
Cuadro 3. Eventos de pérdida de información 27
Cuadro 4. Frecuencia con la que se puede dar el evento 28
Cuadro 5. Impacto - tiempo de suspensión de la operación 28
Cuadro 6. Matriz de calor nivel de riesgo 29
Cuadro 7. Activos de Información 29
Cuadro 8. Amenazas 30
Cuadro 9. Vulnerabilidades 31
Cuadro 10. Consecuencias 34
Cuadro 11. Escalas de probabilidad, impacto y nivel de riesgo 35
Cuadro 12. Niveles de riesgo 39
Cuadro 13. Rango calificación de riesgo 39
Cuadro 14. Evaluación de activos - nivel de riesgo 39
Cuadro 15. Controles seleccionados para los riesgos identificados 41
Cuadro 16. Matriz nivel de riesgo residual 47
Cuadro 17. Convenciones del nivel de cumplimiento de controles 48
Cuadro 18. Evaluación de controles ISO/IEC 27001 49
Cuadro 19. Indicador de estado de controles 58
Cuadro 20. Costo de implantación de control 59
Cuadro 21. Tiempo de implantación 59

Cuadro 22. Tiempo de suspensión de operación.....60
Cuadro 23. Costo - beneficio 60
Cuadro 24. Plan de tratamiento de riesgos.....61
Cuadro 25. Acciones para el mejoramiento de la seguridad de la información 68
Cuadro 26. Actividades plan de toma de conciencia 81
Cuadro 27. Plan de comunicaciones 83

LISTA DE FIGURAS

pág.

Figura 1. Ciclo Demming (PDCA) basado en la norma ISO 27000 22
Figura 2. Proceso de gestión de riesgo en la seguridad de la información 24
Figura 3. Opciones de tratamiento del riesgo 38
Figura 4. Distribución de controles por estado 58

LISTA DE ANEXOS

pág.

ANEXO A. Formato utilizado para el análisis de riesgos 89

ANEXO B. Formato utilizado para el plan de tratamiento 90

ANEXO C. Política de seguridad informática backups 91

ANEXO D. Carta de intención de implementación Tescotur Ltda. 96

GLOSARIO

BACKUP: “se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.”[1].

CONFIDENCIALIDAD: “propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.”[2].

CONTROL: “las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.”[3].

CONSECUENCIA: “indica la acción o situaciones, es un efecto de un determinado suceso, decisión o circunstancia”[4]. En otras palabras, es el resultado de un evento, cuya medición puede darse cualitativa o cuantitativamente.

ESTIMACIÓN DEL RIESGO: “proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable”[5].

EVALUACIÓN DEL RIESGO: “proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo”[6]. Asimismo, es el proceso por el cual se establece la importancia de un riesgo, basados en unos criterios establecidos.

FRECUENCIA: “número de veces que se repite un proceso periódico por unidad de tiempo”[7].

GESTIÓN DEL RIESGOS: “actividades coordinadas para dirigir y controlar una organización con respecto al riesgo”[8].

---

[1] VENERMEDÍA. Definición de backup, 2014 [en línea], disponible en: http://conceptodefinicion.de/backup/

[2] NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). REQUISITOS. (ISO/IEC 27001:2006)

[3] EL PORTAL ISO 27000.ES. ISO 27001, 2012, [en línea], disponible en: http://www.iso27001.es/.

[4] VENERMEDIA. Op cit.

[5] EL PORTAL ISO/IEC 27001. Op. Cit.

[6] NTC-ISO/IEC 27001. Op. Cit. p.3.

[7] Diccionario de la lengua española. Real Academia Española (RAE). Significado frecuencia, 2017, [en línea], disponible en: http://dle.rae.es

[8] NTC-ISO/IEC 27001. Op. Cit. p.3.

IDENTIFICACIÓN DEL RIESGO: proceso por el cual se enumeran y describen los riesgos asociados a la seguridad de la información. “Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.”[9].

IMPACTO: es la consecuencia de la materialización de un riesgo, el cual puede medir el cambio o daño de un activo. “Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos”[10].

ISO: sigla en inglés de la International Organization for Standardization (organización Internacional de normalización)[11].

ISO 27001: “estándar para sistemas de gestión de la seguridad de la información adoptado por ISO, transcribiendo la segunda parte de BS 7799. Es un estándar certificable. Su primera publicación se realizó en el año 2005”[12].

ISO 27002: “código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007”[13].

ISO 27005: “proporciona directrices para la gestión de riesgos de seguridad de la información”[14].

[9] NTC-ISO/IEC 27001. Op. Cit. p.16.
[10] Ibíd., p.5.
[11] ISO. International Organization for Standardization, 2016, [en línea], disponible en: http://www.iso.org/iso/home.html
[12] EL PORTAL ISO 27.000.Op.Cit.
[13] Ibíd.
[14] ISOtools. ISO 27005, 2015, [en línea], disponible en: http://www.isotools.pe/iso-27005-analisis-de-riesgos/

RESUMEN

El proyecto presentado en este documento se enfoca en el análisis de riesgos y su plan de tratamiento para el proceso de backups de la compañía de transportes Tescotur Ltda., en donde a través de un diseño metodológico, se evaluaron los activos de información y se formularon los planes adecuados de tratamiento adaptados a las necesidades de la organización.

Después de realizar la recolección de información con ayuda de las diferentes áreas de la organización, se analizaron las vulnerabilidades, amenazas internas y externas y los impactos que estos tienen sobre los activos de información.

Con base en la norma ISO/IEC 27001 se recomiendan los controles adecuados que permitan mitigar los riesgos que se encuentren fuera de la matriz del nivel aceptable para la organización. Después de esta fase de planeación, se generan las bases para la implementación del sistema de gestión de seguridad de la información.

Palabras clave: Activo, amenaza, control, impacto, ISO 27001, riesgo, seguridad de la información, vulnerabilidad.

INTRODUCCIÓN

Este documento corresponde a la presentación del proyecto de grado, para la obtención del título Especialista en Seguridad Informática. El tema a tratar es diseño y planificación del subsistema de gestión de la seguridad de la información para el proceso de backup, para la empresa de transporte especial de pasajeros Tescotur Ltda., basado en la NORMA ISO/IEC 27000.

La gestión de la seguridad de la información permite a cualquier organización brindar seguridad a su activo más preciado, la información. Por esta razón, se seleccionó esta línea temática para la ejecución del proyecto y se realiza la presentación de las normas ISO escogidas para la planeación del subsistema de gestión de seguridad de la información en la empresa Tescotur Ltda.

Este proyecto nace de la necesidad que tiene la empresa de organizar y proteger la información que se genera diariamente en su operación, dado que no se cuenta con un respaldo en caso de presentarse daños en equipos o pérdidas de información por errores humanos no deseados.

En la organización no se tiene mayor conocimiento sobre la seguridad informática, por lo que, como parte del proyecto, se hace necesario dar a conocer a los directivos la importancia de conocerla y aplicarla de manera efectiva.

Se propone la aplicación de los estándares entregados por la norma ISO/IEC 27001, dado que es la norma que se trabaja en el proceso formativo de la especialización y la más conocida en Colombia en cuanto a seguridad informática.

El proyecto se realiza únicamente sobre el proceso de backup y se limita hasta la fase de planeación, dadas las necesidades inmediatas en la organización, el número de estudiantes que participan en el proyecto y los recursos con los que se cuenta para su ejecución.

1. JUSTIFICACIÓN

Debido al desarrollo tecnológico actual y la importancia de la información para Tescotur Ltda., nace en la organización la necesidad de salvaguardar los respaldos de información (backup), para dar continuidad a las operaciones misionales en caso que se vean afectados negativamente por factores como desastres naturales, ataques malintencionados, robo de hardware, casos fortuitos o intencionados de pérdida de información, entre otros; el establecimiento de medidas de respaldo servirán para garantizar la continuidad en las actividades misionales y por ende continuar en procura de los objetivos del negocio.

En la actualidad la empresa de transporte especial de pasajeros Tescotur Ltda., cuenta con sistemas de información y procesos mejorados, que han incrementado la información administrada de manera notable, haciendo que la administración de los datos sea cada vez más crítica y exigiendo contar con un respaldo eficiente y eficaz, no solo por los factores de riesgo que se ocasionen interna o externamente, si no por lo requisitos legales de mantener la información histórica disponible por varios años.

Este proyecto tiene como finalidad realizar un análisis de riesgo, que permita identificar los activos de información que deben ser tratados en el subsistema de backup, para generar una política que fije las directrices de las actividades de backup, involucrando al personal de la compañía, de tal manera que se salvaguarde la información, manteniéndola integra, confiable y disponible en caso de requerirse su recuperación.

2. DEFINICIÓN DEL PROBLEMA

Tescotur Ltda., es una empresa dedicada a la prestación del servicio de transporte especial de pasajeros, en los últimos años ha realizado cambios importantes a nivel tecnológico, lo que le ha permitido sistematizar sus procesos y dar valor a la información que se genera en sus sistemas de información.

Hoy en día cuenta con diferentes sistemas de software, infraestructura tecnológica y procesos de digitalización de documentos, que buscan organizar la información, todo apoyado en un sistema de gestión de la calidad bajo la norma ISO 9001.

Sin embargo, a pesar de los cambios tecnológicos y de los esfuerzos realizados para mejorar la administración de la información, no se tienen definidos procesos que permitan tener disponible la información en caso de requerirse una recuperación a causa de incidentes adversos como robos, desastres naturales, ciberataques, fallas humanas, entre otras.

Teniendo en cuenta lo anterior, este proyecto diseña y planifica el Subsistema de Gestión de la Seguridad de la Información para el proceso de backup, con la finalidad de lograr que la compañía cuente con la información relevante de una forma íntegra, confiable y disponible en caso de requerirse recuperación ante desastres.

La base fundamental para la ejecución del proyecto se resume en:

2.1 FORMULACIÓN DEL PROBLEMA

¿De qué manera la empresa Tescotur Ltda., puede mejorar sus procesos de Backup para garantizar la disponibilidad, integridad y confidencialidad de la información almacenada?

2.2 OBJETIVOS

2.2.1 Objetivo general. Diseñar y planificar el subsistema de Gestión de la Seguridad de la Información para el proceso de backup, dando una valoración a los activos de información basados en la norma ISO/IEC 27001:2013.

2.2.2 Objetivos específicos.

- Realizar un análisis de riesgo que permita la definición y valoración de los activos de información de la compañía.

- Generar una política de tratamiento de información, para los activos definidos como prioridad en el análisis de riesgo realizado, tomando como base la norma ISO/IEC 27001:2013, para el proceso de backup.

- Definir los roles y responsabilidades en la organización, para la definición del subsistema de gestión de la seguridad de la información para el proceso de backup.

- Socializar la política de tratamiento de información con el personal de la compañía, que hace parte del proceso de backup.

- Definir los controles que se deben implementar en el proceso de backup, teniendo en cuenta la política de tratamiento de información y los análisis de riesgos de seguridad de la información en el mencionado proceso.

2.3 TIPO DE INVESTIGACIÓN

El tipo de investigación aplicado al proyecto es Estudios Explicativos.

2.4 HIPÓTESIS

2.4.1 Hipótesis investigativa (Hi). El diseño y planificación del subsistema de gestión de seguridad de la información para el proceso de backups permitirá que la información se mantenga disponible, integra y confidencial.

2.4.2 Hipótesis nula (Ho). El diseño y planificación del subsistema de gestión de seguridad de la información para el proceso de backups no permitirá que la información se mantenga disponible, integra y confidencial.

2.5 VARIABLES

2.5.1 Variables dependientes.

El cuadro 1. Variables dependientes presenta las variables que se consideraron para la ejecución de este proyecto.

Cuadro 1. Variables dependientes.

No.	Variable	Descripción
1	Diseño	Definir la arquitectura a utilizar para la generación del subsistema de seguridad de la información
2	Planificación	Generar un plan de acción para realizar una tarea o proceso, para este proyecto la realización de un subsistema de seguridad de la información.
3	Backup	Copia de seguridad de la información

Fuente: Elaboración de los autores.

2.5.2 Variables independientes.

EL cuadro 2. Variables independientes presenta las variables que se consideraron para la ejecución de este proyecto.

Cuadro 2. Variables independientes.

No.	Variable	Descripción
1	Norma	Estándar que define los lineamientos que se deben cumplir para la generación de un sistema, para este caso el subsistema de seguridad de la información
2	Empresa	Una organización que desarrolla una actividad económica, sobre un mercado definido, dando satisfacción a la demanda de un grupo de personas u otras organizaciones.

Fuente: Elaboración de los autores.

3. MARCO TEÓRICO

3.1 CONCEPTOS GENERALES

Las empresas existen para crear valor para sus propietarios o accionistas, en consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de gobierno, lo que significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo[15].

La empresa de transportes Tescotur Ltda., dentro de sus metas corporativas tiene como prioridad la satisfacción del cliente, por ende, es necesario realizar un proceso de certificación en las principales normas de calidad para dar garantía y agregar valor a los servicios prestados, cumpliendo estándares que le permiten atender adecuadamente las solicitudes que demandan sus usuarios.

En lo relacionado con las Tecnologías de Información y Comunicaciones (TIC), la empresa de transporte pretende alinearlas con la estrategia del negocio, desarrollando una adecuada gestión de riesgo, especialmente en lo relacionado con la protección de los activos más valiosos, para lo cual pretende diseñar, planificar e implementar el subsistema de Gestión de la Seguridad de la Información para el proceso de backup, permitiendo que la información relevante se encuentre íntegra, confiable y siempre disponible para la adecuada toma de decisiones por parte de la dirección, aun en circunstancias que comprometan la continuidad del negocio, a través de una adecuada gestión de los mismos.

Como primer paso se generará una política general de gestión de seguridad de la información para la empresa de transportes con el fin de lograr comprometer, desde la alta gerencia hasta la base, con la aplicación de la adecuada gestión de seguridad de la información y así poder delimitar la política que se pretende implementar para los backups, esto para asegurar los recursos tanto económicos, humanos y tecnológicos con el fin de llevar a feliz término este proceso.

Se pretende realizar el subsistema de backups tomando como base la norma ISO/IEC 27001:2013, complementando el subproceso con la aplicación de metodología de análisis de riesgos bajo la norma ISO/IEC 27005 dado que está orientada a realizar análisis de riesgos en seguridad de la información.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en continuo desarrollo y actualización- por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commission), que proporcionan un marco de

[15] COBIT 5 ISACA. Directrices para el uso del contenido protegido por derechos de autor [en línea] COBIT © 2012, Estados Unidos. Todos los derechos reservados. Para pautas de uso, ver www.isaca.org/COBITuse.

gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO), la cual especifica los requisitos necesarios para la gestión de la seguridad de la información en cualquier tipo de organización.

La publicación más reciente fue realizada en el año 2013, de donde toma su nombre ISO/IEC 27001:2013. Su primera versión fue publicada en el año 2005 y se basó en la norma británica BS 7799-2.

ISO/IEC 27001 permite que una empresa sea certificada, lo que indica que una entidad de certificación independiente confirma que la seguridad de la información implementada cumple con los lineamientos indicados en la norma.

Por otro lado, la norma ISO/IEC 27005 entrega directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO / IEC 27001 y fue diseñada para la ejecución satisfactoria de seguridad de la información basado en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la norma ISO / IEC 27001 e ISO / IEC 27002 son necesarios para comprender completamente la norma ISO / IEC 27005.

ISO / IEC 27005: 2009, también puede usarse en cualquier tipo de organización tales como empresas comerciales, empresas estatales y organizaciones sin fines de lucro, que deseen gestionar los riesgos que puedan comprometer la seguridad de la información de la organización.

Para el tratamiento del riesgo el proyecto se enfocará en la norma ISO/IEC 27005 la cual ofrece principios y directrices genéricas sobre gestión de riesgos, ya que es la referencia mundial en sistemas de gestión de riesgos, y se eligió teniendo en cuenta que la organización se encuentra en un proceso de recertificación en ISO 9001, siendo necesario ajustar el tratamiento del riesgo con una norma general, sin embargo se tomarán los catálogos de amenazas, vulnerabilidades y valoración de activos contenidos en esta norma para afianzar el proceso de evaluación del riesgo en las TI, enfocados a la gestión de backups.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de Tescotur Ltda., manteniendo un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

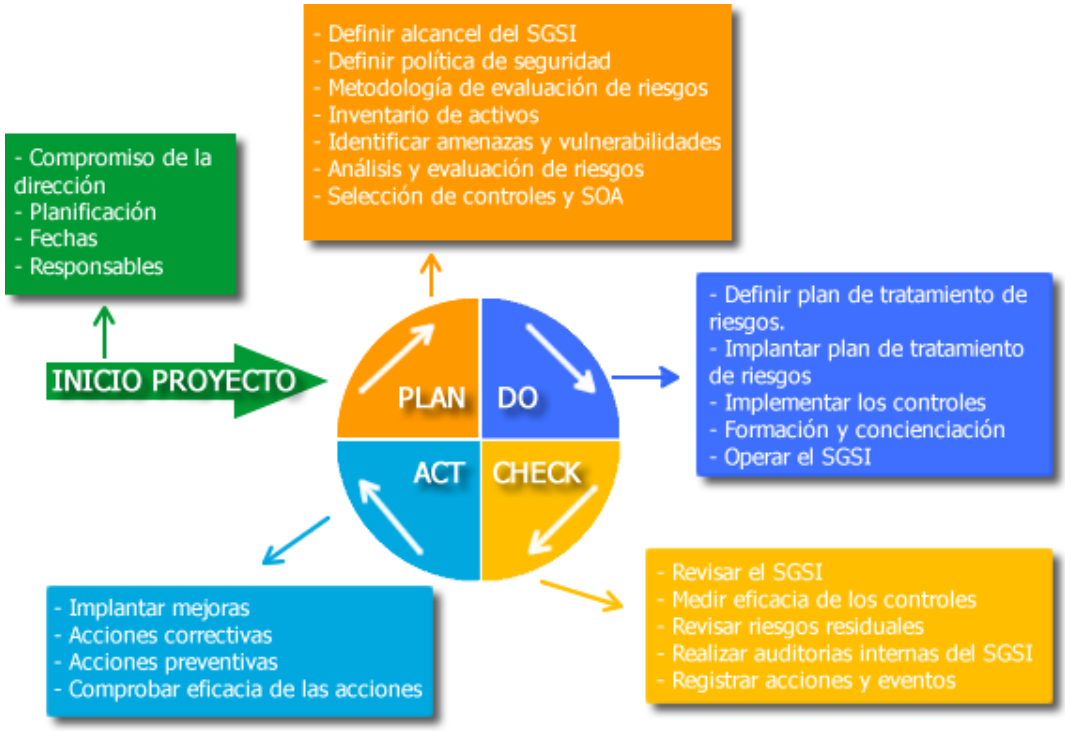
Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA (Plan Do

Check Act por sus siglas en inglés), tradicional en los sistemas de gestión de la calidad.

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI. [4]

Sin embargo y teniendo cuenta el alcance de este proyecto, las fases de Implementar, Verificar y Actuar serán responsabilidad de Tescotur Ltda. La Figura 1. Ciclo Demming (PDCA) basado en la norma ISO 27000, presenta el ciclo PHVA que se aplicará.

Figura 1. Ciclo Demming (PDCA) basado en la norma ISO 27000.



Fuente: Elaboración de los autores.

El hecho de enfocar un SGSI según la norma ISO/IEC 27001 puede aportar las siguientes ventajas a la organización:

– Gestionar un SGSI en una organización, sin importar su tamaño o carácter público o privado.

- Reduce el riesgo de que se produzcan pérdidas de información, con o sin intención.

- Provee estándares para realizar una revisión periódica, que permite la retroalimentación y mejoramiento continuo.

- Establece una metodología clara, entendible para la alta gerencia, permitiendo la toma de decisiones cuando se requiera.

- Contar con el sistema de gestión, obliga a la realización de auditorías externas de manera periódica, permitiendo identificar las incidencias que se pueden presentar, fomentando la mejora continua.

- Permite ofrecer una garantía a clientes y socios estratégicos, dado que muestra a la organización como una entidad que se preocupa por la confidencialidad y seguridad de la información.

- Permite la integración con otros sistemas de gestión normalizados, basados en normas ISO vigentes.

- Ayuda a la organización en el cumplimiento de normas legales vigentes, relacionadas con la información y el manejo de información sensible.

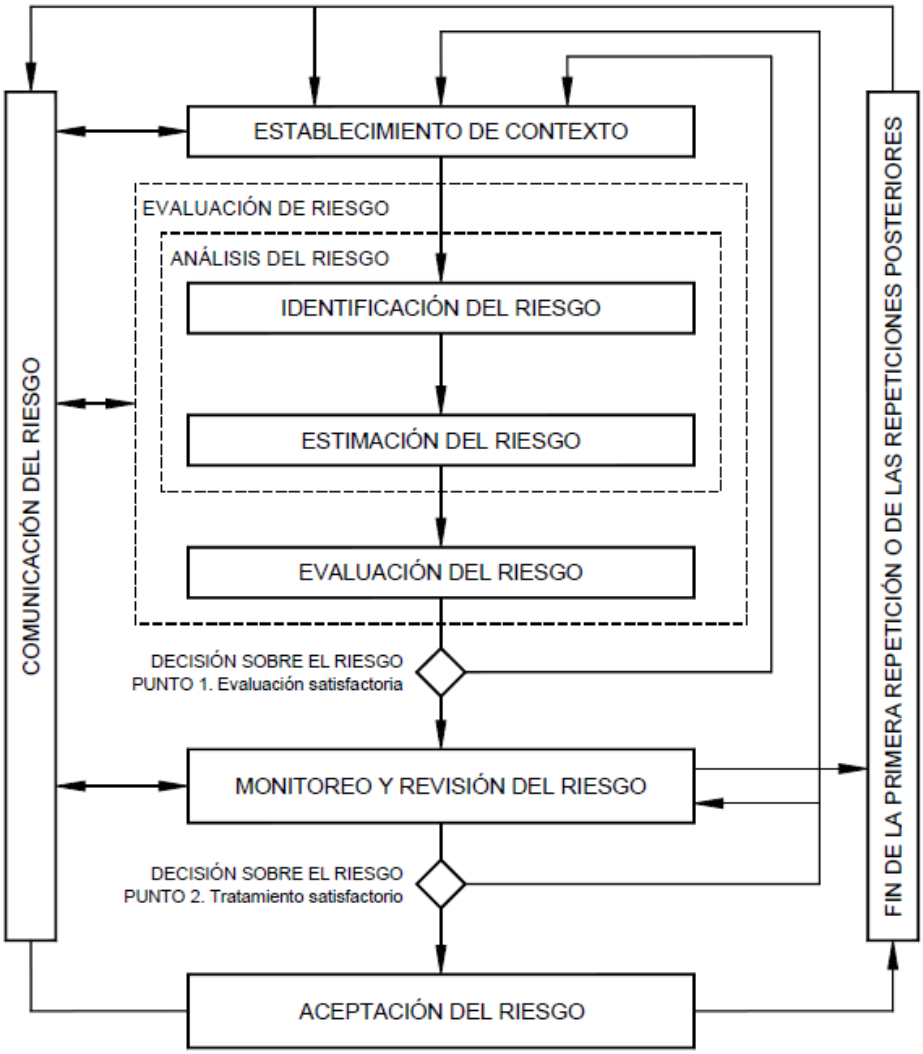
- Mejorar el buen nombre e imagen de la organización, frente a la competencia.

4. METODOLOGÍA

En el desarrollo de este proyecto se trabaja como metodología la norma ISO 27005, en cuanto al análisis de riesgo, dado que esta norma sigue los lineamientos de gestión de riesgo entregados en la norma ISO 27001.

Esta norma se basa en el modelo iterativo que se muestra en la Figura 2. Proceso de gestión de riesgo en la seguridad de la información, en donde se definen las fases a realizar.

Figura 2. Proceso de gestión de riesgo en la seguridad de la información.



Fuente: Figura tomada de la Norma ISO 27005:2009

De acuerdo a esta norma, en el desarrollo de este proyecto se establece el contexto definiendo los criterios de probabilidad, impacto y la matriz de calor correspondiente; posteriormente se realiza la valoración del riesgo mediante la definición de activos, amenazas y vulnerabilidades, con lo que se obtendrán los niveles de riesgo para cada uno de los activos, los cuales serán evaluados para determinar cuáles de estos riesgos son aceptables y cuáles deben ser tratados; finalmente se realiza el plan de tratamiento.

5. DESARROLLO DEL PROYECTO

El proyecto se desarrolla teniendo en cuenta las metodologías descritas en el Capítulo 4 de este documento, a continuación, se describen cada una de las etapas realizadas en el proceso.

5.1 ESTABLECIMIENTO DEL CONTEXTO

5.1.1 Consideraciones generales. Tescotur Ltda., es una empresa dedica a la prestación de servicios de transporte especial de pasajeros, cuya información de operación esta almacenada y administrada en un software Web denominado Sistema ERP.

Adicionalmente, cuenta con un software contable SIIGO en el cual se administra la información financiera de la compañía que, de acuerdo a la normatividad vigente en Colombia, debe mantenerse hasta por 5 años y debe permitir la generación de reportes solicitados por entidades gubernamentales tales como impuestos, información exógena, certificaciones de retenciones, entre otros.

Cada uno de los usuarios del área administrativa tiene a su disposición un equipo de cómputo, desde el cual accede al sistema contable y de operaciones, de acuerdo al cargo asignado en la compañía, además de almacenar la información generada como resultado de las labores realizadas.

Con la información allí almacenada, el usuario genera nueva información de reportes, licitaciones, certificaciones, entre otros.

Por otro lado, de manera reciente la compañía ha decidido adquirir un servidor de impresiones, para la administración de la documentación generada por sus empleados, con el ánimo de controlar el uso de papel y tinta.

Con el subsistema de gestión de seguridad para el proceso de backup, se pretende respaldar la información contenida en los sistemas de información anteriormente mencionados, de tal manera que se garantice la confidencialidad, integridad y disponibilidad de la información cuando esta sea requerida.

5.1.2 Criterios básicos. A continuación, se detallan los criterios de evaluación del riesgo, de probabilidad, impacto y aceptación del riesgo, utilizados para realizar el análisis de riesgos.

5.1.2.1 Criterio de evaluación del riesgo. Para valorar los activos dentro de Tescotur LTDA., es muy importante usar una escala común o criterio semejante,

que permita obtener, a través de un análisis, una valoración correctamente definida que indique la importancia dentro de la empresa.

Para este caso, la valoración de los activos se realiza por aproximación cuantitativa para confidencialidad, integridad y disponibilidad, teniendo en cuenta los diferentes factores que conllevan a mantener la información asegurada bajos las consideraciones de:

- Obligaciones legales.
- Intereses comerciales y económicos.
- Información financiera.
- Información de usuario que genere re-procesos por su no disponibilidad.

5.1.2.2 Criterios de probabilidad. Se solicitó al outsourcing que actualmente presta el servicio de mesa ayuda, la información de los diferentes eventos relacionados con pérdida o modificación de información que se presentan en la compañía, obteniendo el Cuadro 3. Eventos de pérdida de información.

Cuadro 3. Eventos de pérdida de información.

Robo de información
Pérdida de histórico financiero
Daño de disco duro
Manipulación no autorizada de la información
Eliminación de archivos de código fuente
Pérdida de registros
Des configuración de base de datos
Manipulación no autorizada de la información
Eliminación de archivos

Fuente: Elaboración de los autores

Adicionalmente, se revisaron los reportes del último año, sobre los casos atendidos por la mesa de ayuda, para la definición de la frecuencia con la que ocurren estos eventos y se asignó un valor numérico a las frecuencias establecidas, obteniendo el Cuadro 4. Frecuencia con la que se puede dar el evento.

Cuadro 4. Frecuencia con la que se puede dar el evento.

Valoración	Niveles de probabilidad
5	Semanal
4	Mensual
3	Trimestral
2	Semestral
1	Anual

Fuente: Elaboración de los autores

5.1.2.3 Criterios de impacto. Con cada uno de los eventos, se estableció el Cuadro 5. Impacto – Tiempo de suspensión de la operación, la cual indica el impacto que tiene en la compañía la ocurrencia de los eventos, de acuerdo al tiempo de suspensión de las operaciones, que corresponde al tiempo en el que una de las áreas no puede prestar su servicio o un usuario no puede realizar las labores para las cuales fue contratado.

Cuadro 5. Impacto - tiempo de suspensión de la operación.

Valoración	Tiempo
5	Más de 4 semanas
4	4 Semanas
3	2 semanas
2	1 Semana
1	Menos de una semana

Fuente: Elaboración de los autores

5.1.2.4 Criterios de aceptación del riesgo. Los criterios de aceptación de riesgo definidos por Tescotur LTDA., indica sobre qué niveles se deben tratar los riesgos.

En el Cuadro 6. Matriz de calor nivel de riesgo, Los riesgos que se consideran inaceptables están demarcados con el nombre ‘Alto’ y deben ser tratados inmediatamente bajo los procedimientos establecidos para cada uno de ellos; seguido de estos están demarcados los criterios con un nivel ‘Medio’ y ‘Bajo’ cuyo tratamiento está relacionado al control que corresponda, siempre y cuando mitigue el riesgo con un costo/beneficio acorde a los objetivos del negocio.

Cuadro 6. Matriz de calor nivel de riesgo.

Nivel de impacto	Nivel de riesgo				
(5) Más de 4 semanas	5	10	15	20	25
(4) 4 Semanas	4	8	12	16	20
(3)2 semanas	3	6	9	12	15
(2) 1 Semana	2	4	6	8	10
(1) Menos de una semana	1	2	3	4	5
	1 (anual)	2 (semestral)	3 (trimestral)	4 (mensual)	5 (semanal)
	Probabilidad				

Tratamiento	Inaceptables
Medio	Alto
Bajo	

Fuente: Elaboración de los autores

5.2 VALORACIÓN DEL RIESGO

En la realización de la valoración de riesgos se utilizó el formato de Excel presentado en el Anexo A. Formato utilizado para el análisis de riesgos.

5.2.1 Identificación de los activos. De acuerdo al contexto, se define que los activos de información sobre los cuales se realiza el análisis de riesgo, son los relacionados en el Cuadro 7. Activos de información.

Cuadro 7. Activos de Información.

Código	Nombre activo	Responsable	Ubicación	Función
A1	SISTEMA CONTABLE	OUTSOURCING IT	OF. ADMINISTRATIVAS BOGOTÁ	Software de administración de información financiera (SIIGO)
A2	SISTEMA DE OPERACIONES (ERP)	OUTSOURCING IT	OF. ADMINISTRATIVAS BOGOTÁ	Software de administración de información sobre operación de transportes
A3	EQUIPOS USUARIOS	USUARIOS	OF. ADMINISTRATIVAS BOGOTÁ	Información generada por los usuarios, de acuerdo a las labores que realiza en la compañía
A4	SERVIDOR DE IMPRESIONES	OUTSOURCING IT	OF. ADMINISTRATIVAS BOGOTÁ	Administración de colas de impresión, e información de uso de suministros de impresión.

Fuente: Elaboración de los autores

Adicionalmente, se identifican los responsables, la ubicación geográfica y la función de cada activo, para la realización del análisis.

5.2.2 Identificación de las amenazas. La identificación de las amenazas se realizó teniendo en cuenta el reporte entregado por el outsourcing, de los eventos atendidos relacionados con los activos de información definidos en el numeral 5.2.1; y la información entregada mediante entrevista verbal por los usuarios de la compañía.

Se tuvo en cuenta para su definición si los orígenes eran internos o externos, y se usó el catálogo de clasificación de amenazas entregado por la norma ISO 27005.

En el Cuadro 8. Amenazas, se listan las amenazas definidas, incluyendo la identificación del origen y la clasificación dada de acuerdo a la norma.

Cuadro 8. Amenazas.

Amenaza	Origen	Tipo
Usuarios con acceso al sistema	Deliberadas, Accidentales	Personal
Pérdida de suministro de energía	Accidentales	Pérdida de los servicios esenciales
Factores ambientales (Humedad, altas temperaturas)	Ambientales	Ambientales
Personal técnico o de soporte	Deliberadas, Accidentales	Personal
Daños de Hardware	Accidentales	Hardware
Usuarios sin capacitación	Deliberadas, Accidentales	Personal
Espionaje remoto	Deliberadas	Intrusos
Hurto de equipo	Deliberadas	Intrusos
Falla del equipo	Accidentales	Hardware
Mal funcionamiento del equipo	Accidentales	Hardware
Incumplimiento en el mantenimiento del sistema de información	Deliberadas	Software

Fuente: Elaboración de los autores

5.2.3 Identificación de las vulnerabilidades. De acuerdo a la definición de las amenazas conocidas, los activos identificados y los controles existentes, se genera el Cuadro 9. Vulnerabilidades.

Las vulnerabilidades listadas, se definieron mediante el análisis de la información de eventos de seguridad presentados durante el año 2015, entregado por el outsourcing de mesa de ayuda.

Cuadro 9. Vulnerabilidades.

Nombre activo	Amenaza	Control	Vulnerabilidades
SISTEMA CONTABLE	Usuarios con acceso al sistema - Espionaje remoto - Incumplimiento en el mantenimiento del sistema de información	Definición de perfiles de usuario en sistema contable - Definición de roles de usuario en sistema operativo Windows- Generación de backup frecuente.	Facilidad para acceder a los medios de almacenamiento
	Usuarios con acceso al sistema -Incumplimiento en el mantenimiento del sistema de información	Definición de perfiles de usuario en sistema contable - Definición de roles de usuario en sistema operativo Windows- Generación de backup frecuente.	Facilidad para acceder a los medios de almacenamiento
	Pérdida de suministro de energía - Factores ambientales - Personal de soporte técnico - Daños de Hardware -Mal funcionamiento del equipo	Adecuada ventilación en cuarto de servidores - Generación de backup frecuente - Definición de tareas de verificación de funcionamiento de hardware - Mantenimiento preventivo de Hardware - Mantenimiento correctivo de Hardware.	Falta de control de hardware
	Usuarios con acceso al sistema- Espionaje remoto -Incumplimiento en el mantenimiento del sistema de información.	Definición de perfiles de usuario en sistema contable - Definición de roles de usuario en sistema operativo Windows - Mantenimiento preventivos de software (Instalación de actualizaciones y parches) - Capacitación de usuarios en administración y manejo de equipo de cómputo.	Mala Asignación de roles por usuario de TI

Cuadro 9. (Continuación)

Nombre activo	Amenaza	Control	Vulnerabilidades
SISTEMA DE OPERACIONES (ERP)	Personal técnico o de soporte - Espionaje remoto	Definición de roles de usuario en sistema operativo Linux - Definición de roles de usuario FTP - Generación de backup frecuente -Mantenimiento preventivos de software (Instalación de actualizaciones y parches).	Facilidad para acceder a los medios de almacenamiento
	Personal técnico o de soporte - Espionaje remoto - Usuarios sin capacitación	Definición de roles de usuario en software- Definición de roles de usuario en sistema operativo Linux - Definición de roles de usuario FTP - Generación de backup frecuente - Mantenimiento preventivos de software (Instalación de actualizaciones y parches) - Capacitación de usuarios en administración y manejo de equipo de cómputo.	Mala Asignación de roles por usuario de TI
	Personal técnico o de soporte - Incumplimiento en el mantenimiento del sistema de información	Definición de roles de usuario en sistema operativo Linux - Definición de roles de usuario en base de datos - Definición de roles de usuario FTP - Generación de backup frecuente - Mantenimiento preventivos de software (Instalación de actualizaciones y parches).	Mala Asignación de roles por usuario de TI
	Personal técnico o de soporte - Incumplimiento en el mantenimiento del sistema de información - Espionaje remoto - Usuarios sin capacitación.	Definición de roles de usuario en sistema operativo Linux - Definición de roles de usuario en base de datos - Definición de roles de usuario FTP - Generación de backup frecuente - Mantenimiento preventivos de software (Instalación de actualizaciones y parches).	Mala Asignación de roles por usuario de TI

Cuadro 9. (Continuación)

Nombre activo	Amenaza	Control	Vulnerabilidades
SISTEMA DE OPERACIONES (ERP)	Factores eléctricos - Factores ambientales - Personal de soporte técnico - Daños de Hardware	Adecuada ventilación en cuarto de servidores - Generación de backup frecuente - Definición de tareas de verificación de funcionamiento de hardware - Mantenimiento preventivo de Hardware - Mantenimiento correctivo de Hardware	Falta de control de hardware
INFORMACIÓN EQUIPOS FUNCIONARIOS	Usuarios sin capacitación -Personal técnico o de soporte	Capacitación de usuarios en administración y manejo de equipo de cómputo - generación de backup - Roles de usuario en sistema operativo Windows	Manipulación por parte del usuario
	Personal técnico o de soporte - Daños de Hardware - Falla del equipo	Generación de backup - Definición de tareas de verificación de funcionamiento de hardware - Mantenimiento preventivo de Hardware - Mantenimiento correctivo de Hardware	Falta de control de hardware
	Personal técnico o de soporte - Daños de Hardware - Incumplimiento en el mantenimiento del sistema de información	Definición de roles de usuario en sistema operativo Windows - Generación de backup - Capacitación de usuarios en administración y manejo de equipo de computo	Acceso a los equipos por usuarios no autorizados - Falta de control de hardware
SERVIDOR DE IMPRESIONES	Usuarios sin capacitación -Personal técnico o de soporte	Definición de roles de usuario en sistema operativo Windows - Generación de backup - Capacitación de usuarios en administración y manejo de equipo de cómputo - Mantenimiento preventivos de software (Instalación de actualizaciones y parches)	Mala Asignación de roles por usuario de TI
	Factores eléctricos - Factores ambientales - Personal de soporte técnico - Daños de Hardware	Generación de backup - Definición de tareas de verificación de funcionamiento de hardware - Mantenimiento preventivo de Hardware - Mantenimiento correctivo de Hardware	Falta de control de hardware

Fuente: Elaboración de los autores

5.2.4 Identificación de las consecuencias. Las consecuencias listadas en el Cuadro 10. Consecuencias, son el resultado de la evaluación de los eventos de seguridad que se presentaron durante el año 2015, de acuerdo al reporte entregado por el outsourcing, y la verificación de la afectación que tuvieron en los procesos de la empresa.

La afectación fue indicada por los empleados y directivos de la compañía en entrevista verbal; sin embargo, se describen las consecuencias de acuerdo a la categorización realizada por los autores.

Cuadro 10. Consecuencias.

Amenaza	Control	Vulnerabilidades	Consecuencias
Usuarios con acceso al sistema - Espionaje remoto - Incumplimiento en el mantenimiento del sistema de información	Definición de perfiles de usuario en sistema contable - Definición de roles de usuario en sistema operativo Windows- Generación de backup frecuente.	Facilidad para acceder a los medios de almacenamiento	Pérdida de dinero - Incumplimiento con proveedores - Incumplimientos legales
Usuarios con acceso al sistema - Incumplimiento en el mantenimiento del sistema de información	Definición de perfiles de usuario en sistema contable - Definición de roles de usuario en sistema operativo Windows- Generación de backup frecuente.	Facilidad para acceder a los medios de almacenamiento	Incumplimientos Legales
Pérdida de suministro de energía - Factores ambientales - Personal de soporte técnico - Daños de Hardware - Mal funcionamiento del equipo	Adecuada ventilación en cuarto de servidores - Generación de backup frecuente - Definición de tareas de verificación de funcionamiento de hardware - Mantenimiento preventivo de Hardware - Mantenimiento correctivo de Hardware.	Falta de control de hardware	Pérdida de dinero - Incumplimiento con proveedores - Incumplimientos legales
Usuarios con acceso al sistema- Espionaje remoto - Incumplimiento en el mantenimiento del sistema de información	Definición de perfiles de usuario en sistema contable - Definición de roles de usuario en sistema operativo Windows - Mantenimiento preventivos de software (Instalación de actualizaciones y parches) - Capacitación de usuarios en administración y manejo de equipo de cómputo.	Mala Asignación de roles por usuario de TI	Pérdida de dinero - Incumplimiento con proveedores - Incumplimientos legales

Fuente: Elaboración de los autores

5.3 ESTIMACIÓN DEL RIESGO

5.3.1 Metodología para la estimación del riesgo. La metodología para la estimación del riesgo utilizada es cuantitativa, dada la evaluación de los datos históricos sobre los cuales se trabajó el análisis de riesgo entregado por el servicio de outsourcing de mesa de ayuda.

5.3.2 Evaluación de las consecuencias. Dentro de la valoración de los activos de información, se realizó el Cuadro 11. Escalas de probabilidad, impacto y nivel de riesgo.

Cuadro 11. Escalas de probabilidad, impacto y nivel de riesgo.

Activo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de riesgo
SISTEMA CONTABLE	Usuarios con acceso al sistema - Espionaje remoto - Incumplimiento en el mantenimiento del sistema de información.	Facilidad para acceder a los medios de almacenamiento	Pérdida de dinero - Incumplimiento con proveedores - Incumplimientos legales.	2	4	8
	Usuarios con acceso al sistema - Incumplimiento en el mantenimiento del sistema de información.	Facilidad para acceder a los medios de almacenamiento	Incumplimientos legales.	2	4	8
	Pérdida de suministro de energía - Factores ambientales - Personal de soporte técnico - Daños de Hardware -Mal funcionamiento del equipo.	Falta de control de hardware	Pérdida de dinero - Incumplimiento con proveedores - Incumplimientos legales.	1	5	5

Cuadro 11. (Continuación)

Activo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de riesgo
SISTEMA CONTABLE	Usuarios con acceso al sistema- Espionaje remoto -Incumplimiento en el mantenimiento del sistema de información	Mala Asignación de roles por usuario de TI	Pérdida de dinero - Incumplimiento con proveedores - Incumplimientos legales	2	4	8
SISTEMA DE OPERACIONES (ERP)	Personal técnico o de soporte - Espionaje remoto	Facilidad para acceder a los medios de almacenamiento	Retrasos en la prestación del servicio - Disponibilidad del sistema - Pérdida de credibilidad	1	4	4
	Personal técnico o de soporte - Espionaje remoto - Usuarios sin capacitación	Mala Asignación de roles por usuario de TI	Retrasos en la prestación del servicio - Disponibilidad del sistema - Pérdida de credibilidad	2	5	10
	Personal técnico o de soporte - Incumplimiento en el mantenimiento del sistema de información	Mala Asignación de roles por usuario de TI	Retrasos en la prestación del servicio - Disponibilidad del sistema - Pérdida de credibilidad	3	4	12
	Personal técnico o de soporte - Incumplimiento en el mantenimiento del sistema de información - Espionaje remoto - Usuarios sin capacitación	Mala Asignación de roles por usuario de TI	Retrasos en la prestación del servicio - Disponibilidad del sistema - Pérdida de credibilidad	3	4	12

Cuadro 11. (Continuación)

Activo	Amenaza	Vulnerabilidad	Consecuencia	Probabilidad	Impacto	Nivel de riesgo
SISTEMA DE OPERACIONES (ERP)	Factores eléctricos - Factores ambientales - Personal de soporte técnico - Daños de Hardware	Falta de control de hardware	Retrasos en la prestación del servicio - Disponibilidad del sistema - Pérdida de credibilidad	1	5	5
INFORMACIÓN EQUIPOS USUARIOS	Usuarios sin capacitación - Personal técnico o de soporte	Manipulación por parte del usuario	Incumplimientos Legales - Retrasos en la prestación del Servicio	4	3	12
	Personal técnico o de soporte - Daños de Hardware - Falla del equipo	Falta de control de hardware	Incumplimientos Legales - Retrasos en la prestación del Servicio	1	4	4
	Personal técnico o de soporte - Daños de Hardware - Incumplimiento en el mantenimiento del sistema de información	Acceso a los equipos por usuarios no autorizados - Falta de control de hardware	Incumplimientos Legales - Retrasos en la prestación del Servicio - Pérdida de credibilidad	4	4	16
SERVIDOR DE IMPRESIONES	Usuarios sin capacitación - Personal técnico o de soporte	Mala Asignación de roles por usuario de TI	Pérdida de reportes de costos de impresión	1	3	3
	Factores eléctricos - Factores ambientales - Personal de soporte técnico - Daños de Hardware	Falta de control de hardware	Pérdida de reportes de costos de impresión	1	3	3

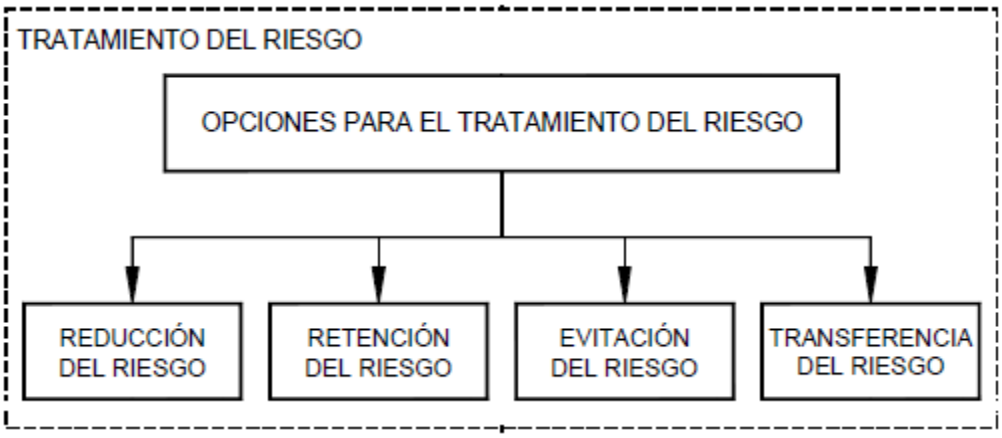
Fuente: Elaboración de los autores

6. TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

6.1 DESCRIPCIÓN GENERAL DEL TRATAMIENTO DEL RIESGO

El principal objetivo del tratamiento, es reducir al máximo los riesgos inaceptables dentro de Tescotur LTDA.; para esto, se cuenta con cuatro opciones de tratamiento que se deberán aplicar de acuerdo al nivel de prioridad y su calificación para cada uno de los riesgos individuales de los activos.

Figura 3. Opciones de tratamiento del riesgo.



Fuente: Figura tomada de la Norma ISO 27005:2009

La norma ISO 27005 maneja 4 opciones de tratamiento del riesgo, como se muestra en la Figura 3. Opciones de tratamiento del riesgo, las cuales se definen de la siguiente forma:

Reducción del Riesgo: Esta opción permite ante la selección de controles adecuados la reducción del riesgo, logrando así que este pueda ser evaluado nuevamente y llevarlo a un nivel aceptable.

Retención del Riesgo: Esta opción está encaminada a tomar una decisión severa donde se definirá si el riesgo es aceptado y este satisface tanto las políticas de seguridad como los criterios de la organización.

Evitación del Riesgo: Esta opción de tratamiento pretende retirar una acción o actividad que se origina a partir de un riesgo dentro de un activo, esto cuando el costo de implementación sobrepasa el beneficio al cual se está aplicando.

Trasferencia del Riesgo: Esta opción busca tener un respaldo y compartir un riesgo con otro grupo o un tercero, de esta forma, este riesgo puede ser minimizado en conjunto, al compartirlo con otros.

Con lo anterior, se establecieron tres niveles de riesgos y su rango de calificación, como se muestra en los Cuadros 12. Nivel de riesgo y Cuadro 13. Rango de calificación de riesgo.

Cuadro 12. Niveles de riesgo.

Tratamiento	Inaceptables
Medio	Alto
Bajo	

Fuente: Elaboración de los autores

Cuadro 13. Rango calificación de riesgo.

Nivel de riesgo	Calificación
ALTO	MAS DE 10
MEDIO	ENTRE 5 Y 9
BAJO	MENOR A 5

Fuente: Elaboración de los autores

Dado el nivel de riesgo obtenido en la evaluación para cada uno de los activos, en el Cuadro 14. Evaluación de activos – Nivel de riesgo, se organizan de mayor a menor nivel de riesgo, con el fin de definir la prioridad de tratamiento.

Cuadro 14. Evaluación de activos - nivel de riesgo.

Nombre activo	Descripción del riesgo	Nivel de riesgo	Criterio de aceptación
INFORMACIÓN EQUIPOS USUARIOS	Manipulación no autorizada de la información	16	Alto - Inaceptable
SISTEMA DE OPERACIONES (ERP)	Desconfiguración de base de datos	12	Alto - Inaceptable
	Manipulación no autorizada de la información	12	Alto - Inaceptable
INFORMACIÓN EQUIPOS USUARIOS	Eliminación de archivos	12	Alto - Inaceptable
SISTEMA DE OPERACIONES (ERP)	Pérdida de registros	10	Alto - Inaceptable

Cuadro 14. (Continuación)

Nombre activo	Descripción del riesgo	Nivel de riesgo	Criterio de aceptación
SISTEMA CONTABLE	Robo de información	8	Medio - Tratamiento
	Pérdida de histórico financiero	8	Medio - Tratamiento
	Manipulación no autorizada de la información	8	Medio - Tratamiento
	Daño de disco duro	5	Medio - Tratamiento
SISTEMA DE OPERACIONES (ERP)	Daño de disco duro	5	Medio - Tratamiento
	Eliminación de archivos de código fuente	4	Bajo - Tratamiento
INFORMACIÓN EQUIPOS USUARIOS	Daño de disco duro	4	Bajo - Tratamiento
SERVIDOR DE IMPRESIONES	Eliminación de archivos	3	Bajo - Tratamiento
	Daño de disco duro	3	Bajo - Tratamiento

Fuente: Elaboración de los autores

6.2 REDUCCIÓN DEL RIESGO

Una vez identificados los niveles de riesgos y teniendo en cuenta la prioridad con la cual van a ser tratados, se definen los controles que se consideran adecuados para reducir el nivel de riesgo, como se muestran en el Cuadro 15. Controles seleccionas para los riesgos identificados. Los controles aplicados se toman del Anexo A de la norma ISO/IEC 27001, de acuerdo a los criterios de aceptación definidos por la organización.

Cuadro 15. Controles seleccionados para los riesgos identificados.

Riesgo	Control ISO 27001	Descripción del control
Pérdida de registros	5.1.1 Políticas para la seguridad de la información.	Se debe definir la política de seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
	6.1.1 Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	7.2.1 Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.
	8.1.2 Propiedad de los activos.	Los activos mantenidos en el inventario deben tener un propietario.
Pérdida de registros	8.1.3 Uso aceptable de los activos.	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de
	9.1.1 Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	9.2.2 Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	9.2.3 Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	9.2.5 Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
	9.2.6 Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	9.4.1 Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Cuadro 15. (Continuación)

Riesgo	Control ISO 27001	Descripción del control
Pérdida de registros	12.3.1 Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	12.4.1 Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Desconfiguración de base de datos	5.1.1 Políticas para la seguridad de la información.	Se definió la política de seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
	6.1.1 Roles y responsabilidades para la seguridad de información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	- Todos los empleados de la organización, y en donde sea pertinente, deben recibir la educación y la formación en toma de conciencia apropiada, actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo.
	9.1.1 Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	9.2.1 Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
	9.2.2 Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	9.2.3 Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	9.4.1 Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Cuadro 15. (Continuación)

Riesgo	Control ISO 27001	Descripción del control
Desconfiguración de base de datos	12.3.1 Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	13.1.1 Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
Manipulación no autorizada de la información	5.1.1 Políticas para la seguridad de la información.	Se definió la política de seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
	6.1.1 Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	7.2.1 Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.
	8.1.2 Propiedad de los activos.	Los activos mantenidos en el inventario deben tener un propietario.
	8.1.3 Uso aceptable de los activos.	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de seguridad de la información
	9.1.1 Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	9.2.1 Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
	9.2.2 Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	9.2.3 Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	9.2.5 Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

Cuadro 15. (Continuación)

Riesgo	Control ISO 27001	Descripción del control
Manipulación no autorizada de la información	9.2.6 Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	9.4.1 Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	12.3.1 Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	12.4.1 Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Eliminación de archivos	5.1.1 Políticas para la seguridad de la información.	Se definió la política de seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
	6.1.1 Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	7.2.1 Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.
	8.1.2 Propiedad de los activos.	Los activos mantenidos en el inventario deben tener un propietario.
	8.1.3 Uso aceptable de los activos.	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de
	9.1.1 Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	9.2.1 Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Cuadro 15. (Continuación)

Riesgo	Control ISO 27001	Descripción del control
Eliminación de archivos	9.2.2 Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	9.2.3 Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	9.2.5 Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
	9.2.6 Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	9.4.1 Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	12.3.1 Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	12.4.1 Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
Manipulación no autorizada de la información	5.1.1 Políticas para la seguridad de la información.	Se definió la política de seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
	6.1.1 Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	7.2.1 Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.

Cuadro 15. (Continuación)

Riesgo	Control ISO 27001	Descripción del control
Manipulación no autorizada de la información	8.1.2 Propiedad de los activos.	Los activos en el inventario deben tener un propietario.
	8.1.3 Uso aceptable de los activos.	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de
	9.1.1 Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	9.2.1 Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
	9.2.2 Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	9.2.3 Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	9.2.5 Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
	9.2.6 Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos, a la información y a las instalaciones de procesamiento de información, se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se realicen cambios.
	9.4.1 Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	12.3.1 Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	12.4.1 Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Fuente: Elaboración de los autores

Una vez aplicados los controles, se obtiene el Cuadro 16. Matriz nivel de riesgo residual, en la que se define el nuevo nivel de riesgo de acuerdo a la mitigación obtenida por los controles.

Cuadro 16. Matriz nivel de riesgo residual.

Nombre activo	Descripción del riesgo	Probabilidad con control	Impacto con control	Nivel de riesgo residual
INFORMACIÓN EQUIPOS USUARIOS	Manipulación no autorizada de la información	3	2	6
SISTEMA DE OPERACIONES (ERP)	Desconfiguración de base de datos	2	2	4
	Manipulación no autorizada de la información	2	1	2
INFORMACIÓN EQUIPOS USUARIOS	Eliminación de archivos	2	2	4
SISTEMA DE OPERACIONES (ERP)	Pérdida de registros	2	1	2

Fuente: Elaboración de los autores

7. DECLARACIÓN DE APLICABILIDAD

A través de esta etapa se evalúa el cumplimento que tiene Tescotur LTDA. en cuanto a la seguridad de la información que contempla los controles bajo la norma ISO/IEC 27001. Dentro del proceso de desarrollo de este proyecto, se han implementado algunas mejoras en los controles, lo que permiten identificar donde se tienen oportunidades de mejora y donde se necesita un mayor grado de concentración con las falencias encontradas.

Para la realización de la evaluación de los controles que están en el Anexo A de la norma ISO/IEC 27001 se debe tener en cuenta el Cuadro 17. Convenciones del nivel de cumplimiento de controles.

Cuadro 17. Convenciones del nivel de cumplimiento de controles.

Nombre	Descripción
Implementado	Control completamente implementado o requiere de mínimas reformas para que se cumpla.
No Implementado	Este control no se encuentra implementado, se debe realizar todo el proceso de implementación.
No Aplica	Este control no aplica a la compañía.

Fuente: Elaboración de los autores

Teniendo en cuenta el Cuadro 17. Convenciones del nivel de cumplimiento de controles, se realiza el diagnostico de los controles bajo la norma ISO/IEC 27001 los cuales describen los 14 dominios de la norma de la siguiente forma:

- Políticas de la seguridad de la información.
- Organización de la seguridad de la información
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía
- Seguridad física y del entorno.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con los proveedores.
- Gestión de Incidentes de seguridad de la información.
- Aspectos de seguridad de la Información de la gestión de la continuidad de negocio.
- Cumplimiento.

7.1 EVALUACIÓN DE CUMPLIMIENTO

En el Cuadro 18. Evaluación de controles ISO/IEC 27001, se evalúa el cumplimiento de cada uno de los controles definidos en los 14 dominios de la norma ISO/IEC 27001 donde se califica su estado de implementación, basados en los parámetros ya establecidos en el Cuadro 17. Convenciones del nivel de cumplimiento de controles.

Cuadro 18. Evaluación de controles ISO/IEC 27001.

Control norma ISO 27001		Estado del control	Justificación
5.1.1	Políticas para la seguridad de la información.	Implementado	Requerido para realizar la revisión de la política de seguridad a través de auditorías e implementación de certificación.
5.1.2	Revisión de las políticas para la seguridad de la información.	Implementado	Requerido para realizar la revisión de la política de seguridad a través de auditorías e implementación de certificación.
6.1.1	Roles y responsabilidades para la seguridad de la información.	Implementado	Requerido para definir los roles y responsabilidades dentro de la organización
6.1.2	Separación de Deberes	No Aplica	No aplica este control dado que el sub-sistema de backup no depende de áreas o dependencias.
6.1.3	Contacto con las autoridades.	No Aplica	No aplica este control dado que el sub-sistema de backup no requiere un contacto con otras autoridades.
6.1.4	Contacto con grupos de interés especial.	No Implementado	Este control es requerido para la notificación de fallas de seguridad a la respectiva área o especialista en seguridad de la información.
6.1.5	Seguridad de la información en la gestión de proyectos.	No Aplica	No aplica este control dado que para el sub-sistema de backup existe una única política de seguridad.
6.2.1	Política para dispositivos móviles	No Aplica	No aplica este control dado que para el sub-sistema de backup no se usan dispositivos móviles.
6.2.2	Teletrabajo.	No Implementado	Este control es requerido para implementar una política de seguridad que permita proteger la información usada por usuarios externos.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
7.1.1	Selección	No Aplica	No aplica este control dado que el sub-sistema de backup no requiere selección de personal.
7.1.2	Términos y condiciones del empleo.	Implementado	Requerido para realizar el proceso de contratación de personal, donde se definen sus responsabilidades con la organización en cuanto a seguridad de la información.
7.2.1	Responsabilidades de la dirección	Implementado	Requerido su uso ya que la Dirección debe exigir a los empleados de la organización el cumplimiento de la seguridad de la información según las políticas establecidas.
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	No Implementado	Este control es requerido para concientizar a los empleados de la organización de la importancia de la seguridad de la información.
7.2.3	Proceso disciplinario.	Implementado	Requerido su uso ya que se debe contar con un proceso disciplinario específico y de notificación a los usuarios, cuando se cometa una violación al sistema de seguridad de la información.
7.3.1	Terminación o cambio de responsabilidades de empleo	Implementado	Requerido su uso ya que se debe notificar al usuario los nuevos roles, cuando se presente cambio en sus responsabilidades o terminación de contrato.
8.1.1	Inventario de activos.	Implementado	Requerido este control para identificar los activos asociados con seguridad de la información en el proceso de backup y su actualización en los documentos de inventarios.
8.1.2	Propiedad de los activos.	No Implementado	Este control es requerido porque se debe asignar un propietario a los activos de información.
8.1.3	Uso aceptable de los activos.	Implementado	Requerido este control para comprometer a los empleados a usar, de manera adecuada, los activos de información.
8.1.4	Devolución de activos.	No Aplica	No aplica este control dado que para el sub-sistema de backup no existe una devolución formal de activos.
8.2.1	Clasificación de la información	Implementado	Requerido este control para identificar la clasificación de la información en el sub-sistema de backup.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
8.2.2	Etiquetado de la información.	No Aplica	La clasificación de backups está contenida en el numeral 8.2.1
8.2.3	Manejo de activos.	Implementado	Requerido este control para el desarrollo e implementación de los procedimientos para el manejo adecuado de activos.
8.3.1	Gestión de medio removibles.	No Aplica	No aplica este control ya que no existe intervención de medios removibles en el proceso de backups.
8.3.2	Disposición de los medios.	No Implementado	Este control es requerido para definir el proceso de forma segura del borrado y formateo de equipos.
8.3.3	Transferencia de medios físicos.	No Aplica	No aplica este control ya que no existe transferencia de medios en la organización para el sub-sistema de backup.
9.1.1	Política de control de acceso.	Implementado	Requerido este control para el correcto acceso a los sistemas de información.
9.1.2	Acceso a redes y a servicios de red	No Aplica	No aplica este control ya que los servicios de backup están enlazados directamente a los equipos de usuario.
9.2.1	Registro y cancelación del registro de usuarios	No Implementado	Este control es requerido para definir cuándo y cómo se realiza la asignación o cancelación de usuarios.
9.2.2	Suministro de acceso de usuarios	No Implementado	Este control es requerido para definir a través de un proceso formal el suministro o revocación de acceso a los sistemas de información.
9.2.3	Gestión de derechos de acceso privilegiado	Implementado	Requerido este control para asignar o restringir privilegios de acceso de usuarios a los sistemas de información
9.2.4	Gestión de información de autenticación secreta de usuarios	No Aplica	No aplica este control ya que para los servicios de backup no se necesita de autenticación secreta para salvaguardar
9.2.5	Revisión de los derechos de acceso de usuarios	Implementado	Requerido este control para verificar los permisos de usuarios a los diferentes sistemas de información.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
9.2.6	Retiro o ajuste de los derechos de acceso	Implementado	Requerido este control para aprobar o denegar los permisos de acceso de los usuarios.
9.3.1	Uso de información de autenticación secreta	Implementado	Requerido este control para garantizar la autenticación de forma secreta de los usuarios a los sistemas de información.
9.4.1	Restricción de acceso a la información	Implementado	Requerido este control para asignar los permisos de acceso a los sistemas de información de acuerdo al rol o responsabilidad del usuario.
9.4.2	Procedimiento de ingreso seguro	Implementado	Requerido este control para asignar métodos de autenticación a los sistemas de información
9.4.3	Sistema de gestión de contraseñas	No Implementado	Este control es requerido para garantizar que las contraseñas de acceso cumplan con los requisitos de seguridad.
9.4.4	Uso de programas utilitarios privilegiados	No Aplica	No aplica este control ya que para el sub-sistema de backup no se requiere instalación de programas utilitarios.
9.4.5	Control de acceso a códigos fuente de programas	Implementado	Requerido este control para revisar los accesos a los códigos fuentes de los sistemas de información.
10.1.1	Política sobre el uso de controles criptográficos	No Aplica	No aplica este control ya que para el sub-sistema de backup no se requiere cifrado.
10.1.2	Gestión de llaves	No Aplica	No aplica este control ya que para el sub-sistema de backup no existen llaves criptográficas.
11.1.1	Perímetro de seguridad física	No Aplica	No aplica este control ya que el proceso se backup se realiza de forma lógica y no física.
11.1.2	Controles de acceso físicos	No Aplica	No aplica este control ya que el proceso se backup se realiza de forma lógica y no física.
11.1.3	Seguridad de oficinas, recintos e instalaciones	No Aplica	No aplica este control ya que el proceso se backup se realiza de forma lógica y no física.
11.1.4	Protección contra amenazas externas y ambientales	Implementado	Requerido este control con el fin de aplicar protección contra ataques malintencionados o accidentales.
11.1.5	Trabajo en áreas seguras	No Aplica	No aplica este control ya que el proceso se backup se realiza de forma lógica y no física.
11.1.6	Áreas de despacho y carga	No Aplica	No aplica este control ya que el proceso se backup se realiza de forma lógica y no física.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
11.2.1	Ubicación y protección de los equipos	No Aplica	No aplica este control ya que el proceso se backup se realiza de forma lógica y no física.
11.2.2	Servicios de suministro	No Implementado	Este control es requerido para garantizar el adecuado backup de los sistemas de información.
11.2.3	Seguridad del cableado.	Implementado	Requerido este control con el fin de proteger la información de interceptaciones, interferencias o daños.
11.2.4	Mantenimiento de los equipos.	Implementado	Requerido este control con el fin de garantizar la disponibilidad e integridad de los equipos de manera continua.
11.2.5	Retiro de activos	No Aplica	No aplica este control ya que el backup no se retira.
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	No Aplica	No aplica este control ya que el backup no se retira.
11.2.7	Disposición segura o reutilización de equipos	No Aplica	No aplica este control ya que para el proceso de backup no se contempla disposición de equipos.
11.2.8	Equipos de usuario desatendido	No Aplica	No aplica este control ya que para el proceso de backup no se contemplan usuarios desatendidos.
11.2.9	Política de escritorio limpio y pantalla limpia	No Aplica	No aplica este control que para el proceso de backup no se contemplan escritorio limpio y pantalla limpia.
12.1.1	Procedimientos de operación documentados	No Aplica	No aplica este control dado que la documentación para el proceso de backup se define en la política, y no se contemplan otros procedimientos para documentar.
12.1.2	Gestión de cambios.	No Aplica	No aplica este control dado que el proceso de backup no contempla cambios en los equipos de usuario.
12.1.3	Gestión de capacidades.	Implementado	Requerido este control con el fin de proyectar cambios en las capacidades de almacenamiento, de acuerdo al crecimiento de la información.
12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	No Aplica	No aplica este control ya que el proceso de backup no contempla desarrollo de software.
12.2.1	Controles contra el código malicioso.	No Implementado	Este control es requerido para detectar y prevenir la propagación de código malicioso.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
12.3.1	Respaldo de la información	Implementado	Requerido este control con el fin de realizar copias de seguridad de la información.
12.4.1	Registro de eventos	No Implementado	Este control es requerido para la revisión regular de los registros de eventos donde se evidencien fallas o intentos de acceso no autorizado.
12.4.2	Protección de la información de registros	No Implementado	Este control es requerido para la revisión regular de los registros donde se evidencien fallas o intentos de acceso no autorizado.
12.4.3	Registros del administrador y del operador	No Implementado	Este control es requerido para la revisión regular de los registros de uso del administrador y operador en los sistemas de información.
12.4.4	Sincronización de relojes.	Implementado	Requerido este control con el fin de tener en la organización una única fuente de sincronización de tiempo.
12.5.1	Instalación del software en sistemas operativos	Implementado	Requerido este control con el fin de garantizar la instalación de parches y actualizaciones de sistema operativo en equipos de usuarios y servidores.
12.6.1	Gestión de las vulnerabilidades técnicas	No Implementado	Este control es requerido para obtener de manera oportuna las vulnerabilidades de los sistemas de información.
12.6.2	Restricciones en la instalación de software.	No Aplica	No aplica este control dado que los usuarios no instalan software para la realización de backup.
12.7.1	Controles de auditoría de los sistemas de información.	No Aplica	No aplica este control dado que el proceso de backup no se audita.
13.1.1	Controles de redes	Implementado	Requerido este control con el fin de proteger la información transmitida por la red local.
13.1.2	Seguridad de los servicios de red	No Aplica	No aplica este control dado que no existen niveles de servicio de red.
13.1.3	Separación en las redes	No Aplica	No aplica este control ya que no existe separación de redes
13.2.1	Políticas y procedimientos de transferencia de información	Implementado	Requerido este control con el fin de garantizar la transferencia de información a través de los medios de comunicación.
13.2.2	Acuerdos sobre transferencia de información	No Aplica	No aplica este control dado que no existe transferencia de información externa.
13.2.3	Mensajería electrónica.	No Aplica	No aplica este control ya que no existe en el proceso de backup mensajería electrónica.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
13.2.4	Acuerdos de confidencialidad o de no divulgación	No Aplica	No aplica este control ya que no existe acuerdos de confidencialidad en el proceso de backup
14.1.1	Análisis y especificación de requisitos de seguridad de la información	No Aplica	No aplica este control ya que para el proceso de backup no existe análisis para equipos de backups
14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	No Aplica	No aplica este control ya que para el proceso de backup no existen llaves publicas
14.1.3	Protección de transacciones de los servicios de las aplicaciones	No Aplica	No aplica este control ya que para el proceso de backup no existen llaves publicas
14.2.1	Política de desarrollo seguro	No Aplica	No aplica este control ya que para el proceso de backup no existen desarrollo
14.2.2	Procedimientos de control de cambios en los sistemas.	No Aplica	No aplica este control ya que para el proceso de backup no existen desarrollo
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	No Aplica	No aplica este control ya que para el proceso de backup no existen aplicaciones
14.2.4	Restricciones en los cambios a los paquetes de software	No Aplica	No aplica este control ya que para el proceso de backup no existen aplicaciones
14.2.5	Principios de construcción de los sistemas seguros	No Aplica	No aplica este control ya que para el proceso de backup no existe desarrollo de aplicaciones
14.2.6	Ambiente de desarrollo seguro	No Aplica	No aplica este control ya que para el proceso de backup no existe desarrollo de aplicaciones
14.2.7	Desarrollo contratado externamente	No Aplica	No aplica este control ya que para el proceso de backup no existe desarrollo de aplicaciones
14.2.8	Pruebas de seguridad de sistemas	No Aplica	No aplica este control ya que para el proceso de backup no existe desarrollo de aplicaciones
14.2.9	Prueba de aceptación de sistemas	No Aplica	No aplica este control ya que para el proceso de backup no existe desarrollo de aplicaciones
14.3.1	Protección de datos de prueba	No Aplica	No aplica este control ya que para el proceso de backup no existen datos de prueba.
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Implementado	Requerido este control con el fin de mitigar los riesgos asociados con los accesos de externos a los activos de información.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Implementado	Requerido este control con el fin de establecer los requisitos de seguridad para acceder, procesar o almacenar información de la organización.
15.1.3	Cadena de suministro de tecnología de información y comunicación	No Aplica	No aplica este control ya que para el proceso de backup no existen suministros.
15.2.1	Seguimiento y revisión de los servicios de los proveedores	Implementado	Requerido este control con el fin de hacer seguimiento y auditar la prestación de servicios con proveedores.
15.2.2	Gestión de cambios en los servicios de los proveedores	No Implementado	Este control es requerido para gestionar cambios en el suministro de servicios, como mantenimientos y mejoras a la política.
16.1.2	Reporte de eventos de seguridad de la información	Implementado	Requerido este control con el fin de tener canales apropiados de comunicación para reportar incidentes de seguridad.
16.1.3	Reporte de debilidades de seguridad de la información	Implementado	Requerido este control con el fin de exigir a los empleados y proveedores notificar de cualquier falla o debilidad en los sistemas de información.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Implementado	Requerido este control con el fin de revisar si una falla o incidencia se cataloga como incidente de seguridad.
16.1.5	Respuesta a los incidentes de seguridad de la información	Implementado	Requerido este control con el fin de dar respuesta a los incidentes de seguridad reportados.
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	Implementado	Requerido este control con el fin de documentar los incidentes de seguridad y usarlos en otras ocasiones para reducir la posibilidad de impacto nuevamente.
16.1.7	Recopilación de evidencias.	No Implementado	Este control es requerido para definir y aplicar procedimientos en la recolección de evidencia y pueda tener una cadena de custodia por parte del área correspondiente.
17.1.1	Planificación de la continuidad de la seguridad de la información.	No Aplica	No aplica este control ya que en el proceso de backup no se garantiza la continuidad del negocio.
17.1.2	Implementación de la continuidad de la seguridad de la información.	No Aplica	No aplica este control ya que en el proceso de backup no se garantiza la continuidad del negocio.

Cuadro 18. (Continuación)

Control norma ISO 27001		Estado del control	Justificación
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	No Aplica	No aplica este control ya que en el proceso de backup no se garantiza la continuidad del negocio.
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Implementado	Requerido este control con el fin de contar con la disponibilidad de los sistemas de información.
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	No Aplica	No aplica para el proceso de backups ya que no existen requisitos legales para su uso.
18.1.2	Derechos de propiedad intelectual	No Aplica	No aplica para el proceso de backups ya que no existen requisitos legales para su uso.
18.1.3	Protección de registros	No Implementado	Este control es requerido para proteger los registros contra pérdida, manipulación o destrucción.
18.1.4	Privacidad y protección de Información de datos personales	No Aplica	No aplica este control para el proceso de backup ya que la política especifica que información se debe salvaguardar.
18.1.5	Reglamentación de controles criptográficos	No Aplica	No aplica este control para el proceso de backup ya que no existen controles criptográficos.
18.2.1	Revisión independiente de la seguridad de la información	Implementado	Requerido este control con el fin de revisar en intervalos planificados los objetivos de control, procedimientos de seguridad de la información, política de seguridad, y validar su implementación.
18.2.2	Cumplimiento con las políticas y normas de seguridad	No Implementado	Este control es requerido para garantizar que los responsables de área ratifiquen que los procesos, políticas y normas de seguridad se cumplan.
18.2.3	Revisión del cumplimiento técnico	No Aplica	No aplica este control para el proceso de backup no existen test técnicos.

Fuente: Elaboración de los autores

7.2 RESULTADOS DE LA EVALUACIÓN DE CUMPLIMIENTO

Una vez detallado cada uno de los controles de la norma ISO/IEC 27001 y su estado actual de implementación, se obtienen los resultados indicados en el Cuadro 19. Indicador de estado de controles.

Cuadro 19. Indicador de estado de controles.

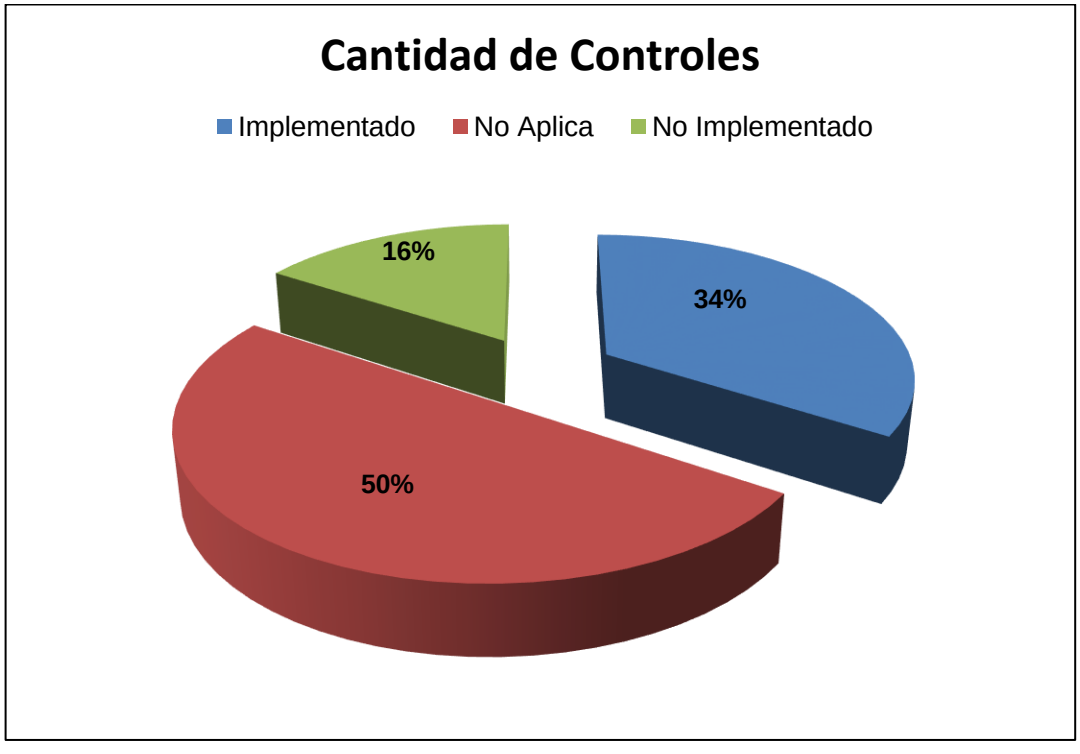
Nivel	Cantidad controles
Implementado	39
No Implementado	18
No Aplica	57

Fuente: Elaboración de los autores

Se puede apreciar que, de los 114 controles, se encontraron 39 controles Implementados en Tescotur LTDA., así mismo 57 controles que no aplican a la organización para el proceso de backups y 18 controles que no están implementados.

La distribución de estos controles dada en porcentajes se muestra en la Figura 4. Distribución de controles por estado.

Figura 4. Distribución de controles por estado.



Fuente: Elaboración de los autores

8. PLAN DE TRATAMIENTO DE RIESGOS

El plan de tratamiento de riesgos tiene como fin dar el tratamiento a los riesgos inaceptables, de acuerdo a los niveles de aceptación determinados por la organización, para su definición se utilizó el formato indicado en el Anexo B. Formato utilizado para el plan de tratamiento

8.1 COSTO – BENEFICIO CONTROLES SELECCIONADOS

La selección de los controles se realiza teniendo en cuenta el costo de la implantación del control, el tiempo de implantación y el nivel de impacto al omitir el control, en cuanto a tiempo de suspensión de la operación.

Para realizar la evaluación de los criterios mencionados, se aplicaron las métricas indicadas en el Cuadro 20. Costo de implantación de control, Cuadro 21. Tiempo de implantación y Cuadro 22 Tiempo de suspensión de operación.

Cuadro 20. Costo de implantación de control.

Valoración	Número de SMMLV (Salario Mínimo Mensual Legal Vigente)
1	Hasta 1 SMMLV
2	Mayor a 1 SMMLV y Hasta 3 SMMLV
3	Mayor a 3 SMMLV y Hasta 7 SMMLV
4	Mayor a 7 SMMLV

Fuente: Elaboración de los autores

Cuadro 21. Tiempo de implantación.

Valoración	Tiempo
1	Hasta 1 Semana
2	Mayor a 1 semana y hasta 4 semanas
3	Mayor a 4 Semanas y hasta 8 Semanas
4	Mayor a 8 Semanas

Fuente: Elaboración de los autores

Cuadro 22. Tiempo de suspensión de operación.

Valoración	Tiempo
1	Menos de una semana
2	1 Semana
3	4 Semanas
4	Más de 4 semanas

Fuente: Elaboración de los autores

Teniendo la valoración de los tres criterios, se calcula un promedio de ((costo de implantación + tiempo de implantación + tiempo de suspensión) /3), el cual indica el costo beneficio, que se evalúa de acuerdo a la métrica indicada en el Cuadro 23. Costo – Beneficio.

Cuadro 23. Costo – beneficio.

Valoración	Costo - beneficio
1	Es superior respecto a los demás controles.
2	Es mayor respecto a los demás controles
3	Es moderado respecto a los demás controles
4	Es menor respecto a los demás controles

Fuente: Elaboración de los autores

8.2 PLAN DE TRATAMIENTO DE RIESGOS Y GUÍA DE IMPLANTACIÓN DE CONTROLES

Teniendo los controles seleccionados, en el Cuadro 24. Plan de tratamiento de riesgos, se detalla el plan propuesto.

Cuadro 24. Plan de tratamiento de riesgos.

Descripción del riesgo	Objetivo	Actividades	Responsable	Tiempo	Recurso / Costo	Controles ISO 27001
Manipulación no autorizada de la información	Mejorar la seguridad de acceso no autorizado al sistema de información	1. Definir perfiles de acceso al sistema, de acuerdo a los roles y responsabilidades indicados en la política de seguridad. 2. Definir proceso para solicitud y asignación de usuarios o perfiles. 3. Configurar el monitoreo de registro de acceso de usuarios al sistema. 4. Realizar copias de seguridad de la información, de acuerdo a lo establecido en la política de seguridad y la política de backups. 5. Configurar el registro de los eventos y fallas de seguridad, de acuerdo a la documentación establecida.	Área de Sistemas	1 Mes	Ingeniero de sistemas Costo: No aplica, ya se cuenta con el personal contratado en la organización.	5.1.1 6.1.1 7.2.1 8.1.2 8.1.3 9.1.1 9.2.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.1 12.3.1 12.4.1

Cuadro 24. (Continuación)

Descripción del riesgo	Objetivo	Actividades	Responsable	Tiempo	Recurso / Costo	Controles ISO 27001
Des configuración de base de datos	Definir los roles de acceso de usuarios internos y externos a la base de datos.	1. Definir perfiles de acceso al sistema de base de datos, de acuerdo a los roles y responsabilidades indicados en la política de seguridad. 2. Definir proceso para solicitud y asignación de usuarios o perfiles. 3. Configurar el monitoreo de registro de acceso de usuarios. 4. Realizar copias de seguridad de la información, de acuerdo a lo establecido en la política de seguridad y la política de backups. 5. Configurar el registro de los eventos y fallas de seguridad, de acuerdo a la documentación establecida.	Administradores	2 semanas	Ingeniero de sistemas Costo: No aplica, ya se cuenta con el personal contratado en la organización.	5.1.1 6.1.1 7.2.2 9.1.1 9.2.1 9.2.2 9.2.3 9.4.1 12.3.1 13.1.1

Cuadro 24. (Continuación)

Descripción del riesgo	Objetivo	Actividades	Responsable	Tiempo	Recurso / Costo	Controles ISO 27001
Eliminación de archivos	Capacitar a los usuarios en el correcto manejo de la información según sus roles de acceso al sistema de información	1. Socializar la política de seguridad a todos los miembros de la compañía. 2. Realizar la configuración de los equipos de cómputo, con creación de usuarios del SO y carpetas de backup, de acuerdo a los roles y responsabilida-des indicados en la política. 3. Definición de manual de funciones, de acuerdo a roles y responsabilida-des establecidos en la política. 4. Explicación a todos los usuarios del plan de comunicaciones para reporte de fallos o eventos de seguridad.	Administrad ores - Área de Sistemas – Recursos Humanos	3 Meses	Ingeniero de sistemas Técnicos en sistemas Coordinador recursos humanos Consultoría profesional en seguridad Costos: contrato de prestación de servicios para la consultoría profesional en seguridad. Valor estimado mensual de servicios, de 4 a 5 millones de pesos.	5.1.1 6.1.1 7.2.1 8.1.2 8.1.3 9.1.1 9.2.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.1 12.3.1 12.4.1

Cuadro 24. (Continuación)

Descripción del riesgo	Objetivo	Actividades	Responsable	Tiempo	Recurso / Costo	Controles ISO 27001
Pérdida de registros	Detectar posibles fallas o manipulación no autorizada de los registros del sistema de información	1. Definir perfiles de acceso al sistema Operativo, Software y Servicio FTP, de acuerdo a los roles y responsabilida-des indicados en la política de seguridad. 2. Definir proceso para solicitud y asignación de usuarios o perfiles. 3. Configurar el monitoreo de registro de acceso de usuarios al Sistema Operativo, Software y Servicio FTP documentación establecida. 4. Definición de frecuencia de actualización de parches de seguridad de sistema operativo y actualización de software entregados por el proveedor.	Área de Sistemas	1 Mes	Ingeniero de sistemas Técnicos en sistemas Costo: No aplica, ya se cuenta con el personal contratado en la organización.	5.1.1 6.1.1 7.2.1 8.1.2 8.1.3 9.1.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.1 12.3.1 12.4.1

Cuadro 24. (Continuación)

Descripción del riesgo	Objetivo	Actividades	Responsable	Tiempo	Recurso / Costo	Controles ISO 27001
Pérdida de registros	Detectar posibles fallas o manipulación no autorizada de los registros del sistema de información	5. Realizar copias de seguridad de la información, de acuerdo a lo establecido en la política de seguridad y la política de backups. 6. Configurar el registro de los eventos y fallas de seguridad, de acuerdo a la documentación establecida.	Área de Sistemas	1 Mes	Ingeniero de sistemas Técnicos en sistemas Costo: No aplica, ya se cuenta con el personal contratado en la organización.	5.1.1 6.1.1 7.2.1 8.1.2 8.1.3 9.1.1 9.2.2 9.2.3 9.2.5 9.2.6 9.4.1 12.3.1 12.4.1

Fuente: Elaboración de los autores

A continuación, se presenta la guía de implantación de los controles seleccionados, de acuerdo a las indicaciones dadas por la norma ISO 27001.

A.5.1.1 Políticas para la seguridad de la información. Este documento contiene los objetivos, alcances, normas, cumplimiento de requisitos legales, de educación, formación y concientización de seguridad de la información relacionada con activos definidos en este proyecto; además de la gestión de continuidad y consecuencias del incumplimiento de la política, complementado con la intención de la dirección en apoyo a las metas de seguridad establecidas.

A.6.1.1 Roles y responsabilidades para la seguridad de la información. Definición de los roles y responsabilidades, de acuerdo a la política de seguridad, asegurando el cumplimiento de los objetivos de seguridad.

A.7.2.1 Responsabilidades de la dirección. Compromiso de la dirección en la exigencia a empleados y contratistas, del cumplimiento de la seguridad de la información de acuerdo a lo establecido en la política.

A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. Realización de jornadas educativas e informativas, cuando ingresen empleados o contratistas nuevos y con frecuencia semestral para empleados y contratistas antiguos, permitiendo que se mantengan informados de las políticas establecidas, sus roles y responsabilidades y el manejo de incidentes.

A.8.1.2 Propiedad de los activos. Definición de los responsables de cada uno de los activos identificados.

A.8.1.3 Uso aceptable de los activos. Definición de los lineamientos de uso de los activos, de acuerdo a la política de seguridad implementada.

A.9.1.1 Política de control de acceso. Definir la política de control de acceso de acuerdo a la clasificación de la información y a la política de seguridad establecida. Esta política de control de acceso debe tener reglas claras de acuerdo a los roles y responsabilidades.

A.9.2.1 Registro y cancelación del registro de usuarios. Definición del proceso de creación y cancelación de usuarios, con acceso a los sistemas de información y backup, para contratistas y empleados de acuerdo a los roles y responsabilidades establecidos.

A.9.2.2 Suministro de acceso de usuarios. Definición de procedimiento para la asignación de acceso de usuarios a los sistemas y servicios, teniendo en cuenta los roles y responsabilidades establecidos.

A.9.2.3 Gestión de derechos de acceso privilegiado. Definición de procedimiento para la asignación de acceso privilegiado, para los usuarios registrados, de acuerdo a los roles y responsabilidades establecidos.

A.9.2.5 Revisión de los derechos de acceso de usuarios. Revisión semestral de los derechos de acceso asignados a los usuarios del sistema, realizada por los propietarios de los activos, de acuerdo a la política establecida.

A.9.2.6 Retiro o ajuste de los derechos de acceso. Procedimiento que establezca los lineamientos necesarios, para realizar el retiro de usuarios o ajuste de los derechos de acceso, una vez se termina la relación por acuerdo o contrato, entre la empresa y empleados o contratistas.

A.9.4.1 Restricción de acceso a la información. Generar las restricciones necesarias para el acceso a la información, de acuerdo a la política de control de acceso establecida por la compañía.

A.12.3.1 Respaldo de la información. Se debe realizar copias de seguridad, de acuerdo a la frecuencia establecida en la política de copias de respaldo, realizando las pruebas de verificación necesarias.

A.12.4.1 Registro de eventos. Realizar el registro de los eventos relacionados con el proceso de backups, mediante logs del sistema operativo y bitácora realizada por el responsable.

A.13.1.1 Controles de redes. Realizar verificación de transferencia de información en la red local trimestralmente, y aplicar las correcciones necesarias cuando sea notificada alguna falla. Aplicar restricciones de acceso a información de dispositivos de almacenamiento de información, de acuerdo a los roles y responsabilidades definidos.

9. OBJETIVOS DE SEGURIDAD DE INFORMACIÓN

Como estrategia para proteger los activos de información de la empresa Tescotur LTDA., es indispensable definir las acciones y responsables de los controles establecidos en la norma ISO/IEC 27001, que permitan el cumplimiento de los siguientes objetivos de seguridad:

- Crear conciencia de la importancia de la seguridad de la información en todos los miembros de la organización, de tal manera que se comprometan en el cumplimiento de las normas establecidas en la política de seguridad.

- Asegurar que la alta gerencia se comprometa en el cumplimiento de la normatividad establecida, exigiendo a todos los miembros de la organización la implementación de los procedimientos establecidos y el buen uso de la información, de acuerdo a los roles y responsabilidades asignados.

- Garantizar que los respaldos de información se realicen bajo los procedimientos establecidos.

- Retroalimentar de manera efectiva el SGSI establecido, permitiendo su mejora continua mediante la identificación de vulnerabilidades y aplicación de controles que permitan su mitigación.

Las acciones definidas tienen la aprobación de la dirección y cuentan con el compromiso de planeación para su seguimiento y cambio a futuro, no todos los controles contenidos en la norma ISO/IEC 27001 requieren acciones para el cumplimiento de los objetivos de seguridad, por lo que en el Cuadro 25. Acciones para el mejoramiento de la seguridad de la información, sólo se indican los controles aplicables, su estado actual y el responsable del control.

Cuadro 25. Acciones para el mejoramiento de la seguridad de la información

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
5.1.1	Políticas para la seguridad de la información.	Implementado	Seguridad	*Control:* Se definió la política de seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
5.1.2	Revisión de las políticas para la seguridad de la información.	Implementado	Seguridad	*Control:* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia
6.1.1	Roles y responsabilidades para la seguridad de la información.	Implementado	Seguridad	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
6.1.4	Contacto con grupos de interés especial.	No Implementado	Seguridad	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad
6.2.2	Teletrabajo.	No Implementado	Seguridad	Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
7.1.2	Términos y condiciones del empleo.	Implementado	RH	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
7.2.1	Responsabilidades de la dirección	Implementado	RH	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.
7.2.3	Proceso disciplinario.	Implementado	RH	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que cometan una violación a la seguridad de la información.
7.3.1	Terminación o cambio de responsabilidades de empleo	Implementado	RH	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
8.1.1	Inventario de activos.	Implementado	RH	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se deben elaborar y mantener un inventario de estos activos.
8.1.2	Propiedad de los activos.	No Implementado	RH	Control: Los activos mantenidos en el inventario deben tener un propietario.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
8.1.3	Uso aceptable de los activos.	Implementado	RH	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
8.2.1	Clasificación de la información	Implementado	RH	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación autorizada.
8.2.3	Manejo de activos.	Implementado	RH	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.3.2	Disposición de los medios.	No Implementado	Sistemas	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
9.1.1	Política de control de acceso.	Implementado	Sistemas	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
9.2.1	Registro y cancelación del registro de usuarios	No Implementado	Sistemas	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.1	Registro y cancelación del registro de usuarios	No Implementado	Sistemas	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.2	Suministro de acceso de usuarios	No Implementado	Sistemas	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
9.2.3	Gestión de derechos de acceso privilegiado	Implementado	Sistemas	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
9.2.5	Revisión de los derechos de acceso de usuarios	Implementado	Sistemas	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
9.2.6	Retiro o ajuste de los derechos de acceso	Implementado	Sistemas	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
9.3.1	Uso de información de autenticación secreta	Implementado	Sistemas	Control: Se debe exigir a los usuarios que cumplan con las prácticas de la organización para el uso de información de autenticación secreta.
9.4.1	Restricción de acceso a la información	Implementado	Sistemas	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
9.4.2	Procedimiento de ingreso seguro	Implementado	Sistemas	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
9.4.3	Sistema de gestión de contraseñas	No Implementado	Sistemas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
9.4.5	Control de acceso a códigos fuente de programas	Implementado	Sistemas	Control: Se debe restringir el acceso a los códigos fuentes de los programas.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
11.1.4	Protección contra amenazas externas y ambientales	Implementado	Seguridad Física	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
11.2.2	Servicios de suministro	No Implementado	Seguridad Física	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
11.2.3	Seguridad del cableado.	Implementado	Sistemas	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se deben proteger contra interceptación, interferencias o daño.
11.2.4	Mantenimiento de los equipos.	Implementado	Sistemas	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
12.1.3	Gestión de capacidades.	Implementado	Sistemas	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido por el sistema.
12.2.1	Controles contra el código malicioso.	No Implementado	Sistemas	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
12.3.1	Respaldo de la información	Implementado	Sistemas	Control: Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
12.4.1	Registro de eventos	No Implementado	Sistemas	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
12.4.2	Protección de la información de registros	No Implementado	Sistemas	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
12.4.3	Registros del administrador y del operador	No Implementado	Sistemas	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
12.4.4	Sincronización de relojes.	Implementado	Sistemas	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
12.5.1	Instalación del software en sistemas operativos	Implementado	Sistemas	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
12.6.1	Gestión de las vulnerabilidades técnicas	No Implementado	Sistemas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
13.1.1	Controles de redes	Implementado	Sistemas	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
13.2.1	Políticas y procedimientos de transferencia de información	Implementado	Sistemas	Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Implementado	Seguridad	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar y se deben documentar.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Implementado	Seguridad	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
15.2.1	Seguimiento y revisión de los servicios de los proveedores	Implementado	Seguridad	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.
15.2.2	Gestión de cambios en los servicios de los proveedores	No Implementado	Seguridad	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de riesgos.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
16.1.1	Responsabilidades y procedimientos	Implementado	Seguridad	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
16.1.2	Reporte de eventos de seguridad de la información	Implementado	Seguridad	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
16.1.3	Reporte de debilidades de seguridad de la información	Implementado	Seguridad	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Implementado	Seguridad	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Implementado	Seguridad	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
16.1.5	Respuesta a los incidentes de seguridad de la información	Implementado	Seguridad	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	Implementado	Seguridad	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto sobre incidentes futuros.
16.1.7	Recopilación de evidencias.	No Implementado	Seguridad	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Implementado	Seguridad	Control: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
18.1.3	Protección de registros	No implementado	Seguridad	Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio

Cuadro 25. (Continuación)

Objetivo de control norma ISO 27001		Estado de control	Área responsable	Control
18.2.1	Revisión independiente de la seguridad de la información	Implementado	Seguridad	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
18.2.2	Cumplimiento con las políticas y normas de seguridad	No Implementado	Seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

Fuente: Elaboración de los autores

10. PLAN DE TOMA DE CONCIENCIA

La norma ISO/IEC 27001 indica que toda la organización debe conocer sus responsabilidades sobre el sistema de seguridad de la información, para esto deben existir tareas definidas donde se determinan las actividades de formación y se establezcan las competencias necesarias para este fin.

La verificación de la formación debe evaluarse de manera individual con el usuario para garantizar que tenga la competencia adecuada de acuerdo a su perfil, rol o responsabilidad en la unidad de negocio, garantizando el cumplimiento de las políticas de seguridad establecidas.

En el Cuadro 26. Actividades plan de toma de conciencia, se propone un plan de toma de conciencia a realizar durante los primeros 6 meses, una vez implementado el SGSI.

Cuadro 26. Actividades plan de toma de conciencia.

Mensaje / Tema	Receptor / Público	Emisor	Acción / Medio	Periodicidad	Verificación / Evaluación
Conocimiento de la política de seguridad	Todos los miembros de la organización	Coordinador de Recursos Humanos	Entrega de una copia de la política de seguridad para lectura personal.	Vinculación de personal (empleados o contratistas) a la compañía	Evaluación escrita sobre los conceptos generales, realizada por recursos humanos. Calificación cuantitativa.
Conocimiento de actualizaciones en la política de seguridad	Todos los miembros de la organización	Profesional en seguridad de la información	Capacitación	Siempre que exista un cambio importante en la política de seguridad	Evaluación escrita sobre los conceptos generales de las modificacio-nes realizadas. Calificación cuantitativa
Administración de información empresarial de acuerdo a las responsabilida-des laborales asignadas	Usuarios y Administradores	Profesional en seguridad de la información, Coordinador de recursos humanos	Manual de funciones, medios impresos, campañas informativas	Mensual	Verificación de manejo de información de acuerdo a normatividad establecida

Cuadro 26. (Continuación)

Mensaje / Tema	Receptor / Público	Emisor	Acción / Medio	Periodicidad	Verificación / Evaluación
Control de acceso	Administrador, RR.HH.	Profesional en seguridad de la información	Conferencia o capacitación	Semestral	Verificación en sitio de aplicación de controles de acceso a áreas restringidas, de acuerdo a la política de seguridad establecida.
Recordación y afianzamiento de conocimiento en seguridad de la información	Todos los miembros de la organización	Profesional en seguridad de la información, coordinador de recursos humanos, administrador de sistemas	Conferencia o capacitación	Trimestral	Actividades didácticas posteriores a la capacitación, que verifiquen los conceptos entregados. Calificación cualitativa.

Fuente: Elaboración de los autores

11. PLAN DE COMUNICACIONES

Con la estrategia de seguridad de la información definida, se plantea un plan de comunicación interna y externa, que permita mantener informado a los responsables de las novedades de seguridad que se puedan presentar, dados los lineamientos establecidos en la política de seguridad.

En el Cuadro 27. Plan de comunicaciones, se detallan las comunicaciones establecidas, con indicación del proceso a realizar.

Cuadro 27. Plan de comunicaciones.

Comunicación	Contenido	Evento	Destinatario	Origen	Proceso
Roles y responsabilidades	Descripción de roles y responsabilidades de acuerdo a las funciones asignadas	Vinculación de personal (empleados y contratistas)	Nuevos miembros de la organización	Recursos Humanos	Entrega de manual de funciones y política de seguridad en medio impreso, con carta de entrega firmada por el funcionario.
Acuerdo de confidencialidad	Documento de acuerdo de confidencialidad, en el que se indica alcance y tiempo de duración.	Vinculación de personal (empleados y contratistas)	Nuevos miembros de la organización	Recursos Humanos	Documento impreso de acuerdo de confidencialidad, debe contener firma de aceptación y debe adjuntarse al contrato laboral.
Convocatoria capacitación	Información de la capacitación, incluyendo tema, duración de la capacitación, horario, lugar y responsable de la capacitación.	Cambio importante en las políticas de seguridad	Todos los miembros de la organización	Profesional en seguridad de la información	Envío de Correo electrónico, con mínimo 2 días de antelación a la realización de la capacitación.

Cuadro 27. (Continuación)

Comunicación	Contenido	Evento	Destinatario	Origen	Proceso
Notificación eventos de seguridad	Detalle del evento de seguridad, de acuerdo a la normativa establecida.	Cuando se presente un evento de seguridad	Responsable, de acuerdo al tipo de evento y normatividad establecida.	Cualquier miembro de la organización.	Notificación al responsable de acuerdo a tipo de evento, con copia a administrado-res y profesional de seguridad encargado del SGSI
Acuerdo de confidencialidad, finalización de contrato.	Documento de acuerdo de confidencialidad, en el que se indica alcance y tiempo de duración.	Finalización de relación laboral con la empresa (empleados y contratistas)	Miembros que finalizan contrato.	Recursos Humanos	Documento impreso de acuerdo de confidenciali-dad, debe contener firma de aceptación y debe adjuntarse al contrato laboral.

Fuente: Elaboración de los autores

12. CONCLUSIONES

Para este proyecto se seleccionó la norma ISO/IEC 27005 como metodología para la realización del análisis de riesgos, como complemento de la norma ISO/IEC 27001, porque explica de manera clara el proceso necesario para la realización de un análisis de riesgos detallado, como se requiere en este caso.

Los controles seleccionados fueron tomados del anexo A de la norma ISO/IEC 27001, dado que entrega controles estandarizados y clasificados, que permite identificar de manera clara y fácil los riesgos que pueden ser reducidos con su aplicación.

Durante el levantamiento de información para la realización del análisis de riesgos, se pudo identificar que en la compañía no estaban plenamente definidos los roles y responsabilidades de empleados y contratistas; sin embargo, gracias a este análisis la compañía logró identificarlos e implementarlos antes de completar el proceso de análisis de riesgos, como se evidencia en la política de seguridad que se encuentra en el Anexo C. Política de seguridad informática backups.

Con la realización del análisis de riesgo, se encontró que la empresa ha venido implementando controles de seguridad, sin tener conocimiento previo sobre los estándares o metodologías propias de la seguridad en la información. Estos controles se han aplicado basados únicamente en las necesidades tecnológicas de la organización, y en su mayoría sugeridas por el outsourcing de tecnología actualmente contratado.

Con la realización de este proyecto, los directivos de la empresa participaron activamente y dieron a conocer su interés en continuar con el proceso para llegar a la implementación del sistema de seguridad propuesto, además de identificar otros procesos en los cuales se requiere el diseño e implementación de un SGSI siguiendo los lineamientos de la norma ISO/IEC27001.Esto se demuestra con la carta de intención entregada por la compañía a los autores, la cual se encuentra en el Anexo D. Carta de intención de implementación Tescotur Ltda.

Con la realización del análisis de riesgos, los directivos se dieron cuenta de los fallos de seguridad con los cuales han venido trabajando, incluso que no son propios del subproceso de backup, y entendieron que la implementación de un SGSI en la organización es realmente una inversión, que, aunque no generará dinero, si permitirá preservar su prestigio y buen nombre, además de ahorrar en costos en los que puedan incurrir en el caso de explotarse una vulnerabilidad.

Con el desarrollo del proyecto también se evidenció, que las principales vulnerabilidades vienen de los empleados de la organización. Con la realización de las jornadas de concientización, se logró que los empleados y directivos vieran la importancia de una buena administración de la información.

A través de la realización de este proyecto en la organización, los empleados que participaron en el levantamiento de información, lograron darse cuenta que muchos de los fallos de seguridad que se pueden presentar en una organización, tienen origen en las acciones cotidianas de cualquier persona, tales como prestar contraseñas por “ayudar” a un compañero de trabajo, o compartir el formato de un documento que sin darse cuenta contiene información de la cual solo él es responsable.

13. RECOMENDACIONES

Los directivos de Tescotur Ltda., dieron a conocer su interés en completar el proceso de implementación del sistema de gestión de seguridad de la información propuesto en este proyecto, por lo cual se realizaron las siguientes recomendaciones, para que se logre este objetivo.

- Los controles sugeridos deben ser implementados en un lapso no mayor a un año, tiempo que se calcula teniendo en cuenta la proyección de recursos de información identificados durante la realización del proyecto.

- En la actualidad la empresa cuenta únicamente con un outsourcing en sistemas que da apoyo a los requerimientos tecnológicos, sin embargo, y dado su interés en la implementación del SGSI propuesto, la empresa debe contar con personal especializado en seguridad de la información, que conozca la norma ISO/IEC 27001 para que pueda alinear los objetivos de negocio con los objetivos de seguridad de la información, y llevar a buen término la implementación del SGSI.

- Dado el análisis de costo-beneficio realizado para la definición de los controles a implementar, los directivos con el apoyo de un especialista en seguridad de la información, puede definir la prioridad de implementación de cada uno de los controles de acuerdo a sus necesidades y recurso económico.

BIBLIOGRAFÍA

COBIT 5 ISACA. Directrices para el uso del contenido protegido por derechos de autor [en línea] COBIT © 2012, Estados Unidos. Todos los derechos reservados. Para pautas de uso, ver www.isaca.org/COBITuse.

EL PORTAL ISO 27.000.ES. ISO 27001, 2012, [en línea], disponible en: http://www.iso27001.es/

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma técnica Colombiana para la presentación de tesis, trabajos de grado, y otros trabajos de investigación. Bogotá D.C., ICONTEC, 2008. (NTC 1486).

_____. Norma técnica Colombiana para referencias documentales para fuentes de información electrónica. Bogotá D.C., ICONTEC, 1998. (NTC 4490).

_____. Norma técnica Colombiana para referencias bibliográficas, contenidos, forma y estructura. Bogotá D.C., ICONTEC, 2008. (NTC 5613).

_____. Norma Técnica Colombiana Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. (ISO/IEC 27001:2006).

ISO. International Organization for Standardization, 2016, [en línea], disponible en: http://www.iso.org/iso/home.html

ISOtools. ISO 27005, 2015, [en línea], disponible en: http://www.isotools.pe/iso-27005-analisis-de-riesgos/

REAL ACADEMIA ESPAÑOLA (RAE). Diccionario de la lengua española. Significado frecuencia, 2017, [en línea], disponible en: http://dle.rae.es

VENERMEDÍA. Definición de backup, 2014 [en línea], disponible en: http://conceptodefinicion.de/backup/

ANEXOS

ANEXO A. FORMATO UTILIZADO PARA EL ANÁLISIS DE RIESGOS

CÓDIGO	NOMBRE ACTIVO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	AMENAZA	CONSECUENCIAS	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	CONTROL	PROBABILIDAD CON CONTROL	IMPACTO CON CONTROL	NIVEL DE RIESGO CON CONTROL

Fuente: Elaboración de los autores

ANEXO B. FORMATO UTILIZADO PARA EL PLAN DE TRATAMIENTO

Descripción del riesgo	Objetivo	Actividades	Responsable	Tiempo	Recurso / Costo	Controles ISO 27001

Fuente: Elaboración de los autores

ANEXO C. POLÍTICA DE SEGURIDAD INFORMÁTICA BACKUPS

	**TESCOTUR LTDA.**	Fecha de Aplicación:
	POLÍTICA DE SEGURIDAD INFORMÁTICA BACKUPS	Versión: 001

PROPÓSITO

El propósito de esta política es contribuir al logro de una seguridad informática dentro de la empresa, un uso apropiado y un mayor aprovechamiento de los datos, la información y un correcto sistema de backups dentro de TESCOTUR LTDA.

En particular, los objetivos comprenden:

• Asegurar que la información de la compañía almacenada por cada uno de los usuarios en los equipos de cómputo asignados, en la carpeta compartida bajo el nombre de “Backup”, los servidores de software ERP, SIIGO y servidor de Impresión, tenga su respectivo proceso de respaldo el cual será almacenado en un medio local.

• Asegurar que los recursos tecnológicos de respaldo de información (backups), al servicio de TESCOTUR LTDA., se utilicen en forma consistente con la misión de TESCOTUR LTDA. y que se haga de una manera ética, legal, honrada, considerada, responsable y apropiada, de conformidad con éstas y otras políticas institucionales y leyes aplicables existentes.

• Asegurar que la información salvaguardada en los diferentes sistemas de backups implementados en TESCOTUR LTDA., operen de manera correcta y sin interrupciones o perturbaciones al trabajo realizado día a día por los funcionarios.

• Dar a conocer a los usuarios la importancia de esta política de backups y el correcto uso de su procedimiento para garantizar un respaldo óptimo dentro de TESCOTUR LTDA.

ALCANCES

La política aplica al uso y funcionamiento de los recursos informáticos para el proceso de backups que se encuentran al servicio de TESCOTUR LTDA., sean o no de propiedad de TESCOTUR LTDA., sea que estén compartidos o controlados individualmente, sea que estén aislados o interconectados a redes. Los recursos

incluyen los datos y la información de los usuarios, el software y los equipos de cómputo y comunicaciones. Las políticas aplican a funcionarios, contratistas y otros usuarios quienes, contando con la debida autorización, requieran el proceso de respaldo de información al servicio de TESCOTUR LTDA.

USO APROPIADO DE LA POLÍTICA

El uso de los sistemas de respaldo de información, backups, y servicios asociados que se proporcionan a los usuarios debe ser consistente con los fines de TESCOTUR LTDA., igual que ocurre con cualquier otro recurso que se suministra como herramienta de trabajo. El estándar de conducta respecto al uso de los recursos informáticos es similar al estándar general de conducta que se espera de los empleados y otros usuarios autorizados respecto al uso de información confidencial, interna o de uso dentro de la empresa. El uso debe ser ético, legal, honrado, racional, eficiente, responsable, considerado con el trabajo y derechos de otros, y respetuoso de los derechos de autor y de los mecanismos de seguridad y de control impuestos. Se espera que las personas actúen responsablemente con la clasificación de la información almacenada dentro de los sistemas de backups implementados y deberán ser responsables de sus acciones, de igual manera como si ellos estuvieran tratando con otros medios tradicionales.

RESPONSABILIDADES

Usuario

• Es responsabilidad de cada usuario almacenar la información que se desea salvaguardar en la carpeta compartida que se encuentra en cada uno de sus computadores o estación de trabajo llamada “Backup”, de tal manera que se garantice la realización de la copia de respaldo a los servidores destinados para este fin.

• Notificar a las personas de sistemas o administradores, el no funcionamiento o falta de carpetas para la correcta ejecución de las actividades de backups.
• Es deber de todo usuario reportar a la mesa de ayuda de TESCOTUR LTDA., cualquier uso inapropiado de los recursos, incidentes o eventos que puedan afectar el normal procesamiento de backups o pérdida de información.

• Seguir las políticas de seguridad y procedimientos para su uso.

Administradores

• El Administrador de la Red debe hacer la retención de las copias de respaldo de acuerdo como se encuentra indicado en la política de respaldo de información.

• Verificar desde el servidor de Backup que se hayan realizado las copias de cada equipo, de acuerdo a la política de respaldo de información establecida en la compañía.

• Configurar los equipos de cómputo para realizar el backup de acuerdo a la política de respaldo establecida por TESCOTUR LTDA.

• Los administradores de sistemas de información, deben cumplir las políticas de control de acceso a la información y criterios de clasificación de información definidos en la política de respaldo establecida.

• Actualizar y mantener al día los servidores de backups con sus respectivos parches de seguridad.

• Obrar con ética y profesionalismo en el cumplimiento de su deber, velando al máximo por la privacidad y confidencialidad de la información.
RR.HH.

• Capacitarse y mantenerse actualización sobre la política de backups establecida por TESCOTUR LTDA.

• Dar a conocer, promover y capacitar al nuevo personal que ingrese a la empresa del procedimiento y política de backups implementado.

• Participar en las actividades institucionales que se programen sobre política y gestión de respaldo de la información.

RESPALDOS

La información almacenada en las carpetas de backup y los diferentes servidores implementados serán respaldados periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.

• Los equipos de cómputo asignados al personal de la compañía, contienen el directorio identificado con el nombre “backup”.

• Se realizará backup de los documentos de la empresa que estén almacenados en la carpeta de backups de cada uno de los equipos de cómputo.

• No se realizará backup de los documentos de carácter personal o individual
En principio dicho directorio solo contempla la presencia de datos sensibles e información de la compañía, no personal. El backup de estos (documentos personales) queda bajo la responsabilidad del usuario del puesto de trabajo.

- Los respaldos de información y aplicaciones estarán alojados en un servidor único destinado solo al proceso de backups.

- Para reforzar la seguridad de la información, los usuarios deberán hacer respaldos de la información en la carpeta destinada para este fin, dependiendo de la importancia y frecuencia de cambio; la información almacenada en estos medios, serán responsabilidad absoluta de los usuarios.

- Los administradores de los medios de almacenamiento de backup a través del monitoreo constante a las carpetas salvaguardadas en el servidor de backup, deberán reportar a la mesa de ayuda cualquier incidente de seguridad que atente contra la integridad, disponibilidad y confidencialidad de los archivos.

- La periodicidad con la que se realicen las sincronizaciones con la carpeta de almacenamiento de backups de usuario y servidor, deben realizarse de acuerdo a la política de respaldo actualmente definida en la compañía.

- La periodicidad con la que se realicen las sincronizaciones con los servidores de aplicaciones y funciones (ERP, SIIGO e Impresión) y servidor, deben realizarse de acuerdo a la política de respaldo actualmente definida en la compañía.

HERRAMIENTAS

Las herramientas nos permiten implementar la política de backup. Dada la variedad de plataformas que manejamos hoy en día, para cumplir con los backups estipulados usaremos software:

Duplicity: es una aplicación libre para sistemas de tipo Unix y Microsoft Windows que ofrece transmisión eficiente de datos incrementales, que opera también con datos comprimidos y cifrados. Mediante una técnica de delta encoding, permite sincronizar archivos y directorios entre dos máquinas de una red o entre dos ubicaciones en una misma máquina, minimizando el volumen de datos transferidos. La duplicidad diseña un esquema en el que el primer archivo es una copia de seguridad completa (full) y posteriores (incrementales) copias de seguridad sólo se suman las diferencias desde la última copia de seguridad completa o incremental.

CUMPLIMIENTO

Cualquier funcionario u otro usuario que haya violado esta política de backups y dentro de sus labores necesiten la restauración de la información y no esté disponible, puede quedar sujeto a una acción disciplinaria.

DEFINICIONES

Administrador: Término utilizado para hacer referencia a todas aquellas personas responsables por la operación día a día de un sistema de cómputo o recursos de una red de cómputo.

Confidencialidad: Característica de los datos y la información de ser revelados únicamente a personas o entidades autorizadas, en la forma y horarios autorizados.

Datos: Representación de hechos, conceptos o instrucciones en una manera formal, apropiada para comunicación, interpretación o procesamiento manual o automático.

Datos personales: Información que identifica o describe a un individuo.

Deber: Una obligación moral o instituida

Funcionario: Por facilidad, se utiliza este término para hacer referencia a cualquier persona perteneciente a la planta de personal de TESCOTUR o con un nombramiento provisional.

Información: Es el significado asignado a los datos por medio de convenciones aplicadas a ellos.

Política: Es una declaración formal de las reglas o normas que los usuarios de los recursos tecnológicos y de información de una organización deben acatar.
Responsabilidad: Cargo u obligación moral de responder por un posible error en una cosa o asunto determinado.

Seguridad: Medidas tomadas para reducir el riesgo de 1) acceso y uso no autorizado 2) daño o pérdida de los recursos, por algún desastre, error humano, fallo en los sistemas, o acción maliciosa.

Servidor: Computador no necesariamente multiusuario/multitarea que desempeña una función específica, generalmente en forma dedicada y desatendida. En un servidor no trabajan los usuarios

Sistema: Término genérico utilizado por brevedad para hacer referencia a sistema de información.

Usuario: Término utilizado por brevedad para referirse a usuario autorizado.

Fuente: Elaboración de los autores

ANEXO D. CARTA DE INTENCIÓN DE IMPLEMENTACIÓN TESCOTUR LTDA.

Servicio Amable

tescotur S.A.
RESPONSABILIDAD Y CUMPLIMIENTO
Vehículos de gran Gama y Condiciones para
Transporte Especial de Colegios, Empresas y
Turismo a nivel Local y Nacional.

Bogotá D.C., 15 de diciembre de 2016.

Señores
UNIVERSIDAD PILOTO DE COLOMBIA
DIRECCION DE POSTGRADOS
Ciudad

Asunto: INTERES EN PROYECTO DE GRADO DISEÑO Y PLANIFICACIÓN DEL SUB-SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE BACKUPS BASADA EN LA NORMA ISO/IEC 27000 EN LA EMPRESA DE TRANSPORTE ESPECIAL DE PASAJEROS TESCOTUR LTDA. INGENIEROS NICOLAS MURILLO Y VIVIANA FARFAN.

Respetados Señores.

Por medio de la presente queremos dar a conocer nuestro interés en implementar el Sub-Sistema de gestión de seguridad de la información para el proceso de backups, planteado por los ingenieros Nicolás Murillo y Viviana Farfan, en su proyecto de grado para optar al título de Especialista en Seguridad informática.

Durante el desarrollo del proyecto nos han dado a conocer todo el proceso, permitiéndonos identificar la importancia de la seguridad de la información para nuestra organización, es por esto que les hemos dado a conocer nuestro interés de realizar la implementación del sistema propuesta, como fase inicial para continuar ampliando el sistema de seguridad para otras áreas y procesos de la organización.

Agradecemos el trabajo realizado por los ingenieros, y la oportunidad dada por la universidad de participar en estos procesos de formación.

Cordialmente,

Ing. JAIME DERCH MASSANET
DIRECTOR COMERCIAL Y OPERATIVO
TESCOTUR S.A.

BUREAU VERITAS Certification

Transportes Especiales Colegios y Turismo "TESCOTUR S.A." - NIT. 860.517.112-7 - www.tescotur.com
Oficinas: Carrera 68 C No. 74 B 15, Bogotá, COL. / Fax: (57)(1) 755 0137 * PBX: (57)(1) 742 7600

Fuente: Tescotur Ltda.

DISEÑO Y PLANIFICACIÓN DEL SUB-SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE BACKUPS BASADA EN LA NORMA ISO/IEC 27000 EN LA EMPRESA DE TRANSPORTE ESPECIAL DE PASAJEROS TESCOTUR LTDA

Viviana Farfan, Nicolas Murillo
viviaf01@gmail.com, nicolasmurillo.17@gmail.com
Universidad Piloto de Colombia
Bogotá D.C, Colombia

***Resumen*— El proyecto presentado en este documento se enfoca en el análisis de riesgos y su plan de tratamiento para el proceso de backups de la compañía de transportes Tescotur Ltda, en donde a través de un diseño metodológico, se evaluaron los activos de información y se formularon los planes adecuados de tratamiento adaptados a las necesidades de la organización.**

Después de realizar la recolección de información con ayuda de las diferentes áreas de la organización, se analizaron las vulnerabilidades, amenazas internas y externas y los impactos que estos tienen sobre los activos de información.

Con base en la norma ISO/IEC 27001 se recomiendan los controles adecuados que permitan mitigar los riesgos que se encuentren fuera de la matriz del nivel aceptable para la organización. Por consiguiente, después de esta fase de planeación, se generan las bases para la implementación del sistema de gestión de seguridad de la información.

***Palabras Clave*—Activo, amenaza, control, impacto, mitigación, riesgo, vulnerabilidades.**

Abstract— The project presented in this document focuses on risk analysis and its treatment plan for the backup process of the transportation company Tescotur Ltda, where through a methodological design, the information assets were evaluated and the Adequate treatment plans tailored to the needs of the organization.

After collecting information with the help of the different areas of the organization, vulnerabilities, internal and external threats and their impact on information assets were analyzed.

Based on ISO / IEC 27001, suitable controls are recommended to mitigate risks outside the matrix of the level acceptable to the organization. Consequently, after this planning phase, the bases for the implementation of the information security management system.

***Index Terms*— Active, threat, control, impact, mitigation, risk, vulnerabilities.**

I. INTRODUCCION

La información en el mundo de hoy es uno de los activos más importante para las organizaciones, es por esto que se deben contemplar medidas de aseguramiento contra las distintas amenazas que se encuentran presentes tanto internas como externas en las organizaciones.

Uno de los principales objetivos para la organización radica en proteger su información, para esto se ha invertido en costos y tiempo para levantar una infraestructura técnica que permita salvaguardar la información, pero como sucede en muchas organizaciones no tienen ninguna política o procedimientos establecidos que ayuden a hacer un seguimiento de control a los activos de información.

Con la elaboración de este proyecto, se realiza un análisis de riesgos para el proceso de backup de la empresa de transportes especial de pasajeros Tescotur Ltda, el cual permite revelar las vulnerabilidades, amenazas y riesgos a los cuales están expuestos los diferentes activos de información de la organización.

Posteriormente al análisis de riesgos realizado a la organización siguiendo la metodología establecida en la norma ISO/IEC 27001:2013, se podrá evidenciar los activos de información que se encuentran en riesgo y de esta forma proyectar un plan de tratamiento que busque mitigarlos por medio de los controles planteados en la ISO/IEC 27001:2013 en su anexo A.

II. PLANTEAMIENTO DEL PROBLEMA

Tescotur Ltda es una empresa dedicada a la prestación del servicio de transporte especial de pasajeros, en los últimos años ha realizado cambios importantes a nivel tecnológico, lo que le ha permitido sistematizar sus procesos y dar valor a la información que se genera en sus sistemas de información.

Hoy en día cuenta con diferentes sistemas de software, infraestructura tecnológica y procesos de digitalización de documentos, que buscan organizar la información, todo apoyado en un sistema de gestión de la calidad bajo la norma ISO 9001.

Sin embargo, a pesar de los cambios tecnológicos y de los esfuerzos realizados para mejorar la administración de la información, no se tienen definidos procesos que permitan

tener disponible la información en caso de requerirse una recuperación, a causa de incidentes adversos como robos, desastres naturales, ciberataques, fallas humanas, entre otras.

Teniendo en cuenta lo anterior, este proyecto diseña y planifica el subsistema de Gestión de la Seguridad de la Información para el proceso de backup, con la finalidad de lograr que la compañía cuente con la información relevante de una forma íntegra, confiable y disponible en caso de requerirse recuperación ante desastres.

La base fundamental para la ejecución de este proyecto es:

¿De qué manera la empresa Tescotur Ltda puede mejorar sus procesos de Backup para garantizar la disponibilidad, integridad y confidencialidad de la información almacenada?

III. OBJETIVOS

a. Objetivo General

Diseñar y planificar el subsistema de Gestión de la Seguridad de la Información para el proceso de backup, dando una valoración a los activos de información basados en la norma ISO/IEC 27001:2013.

b. Objetivos Específicos

✓ Realizar un análisis de riesgo que permita la definición y valoración de los activos de información de la compañía.

✓ Generar una política de tratamiento de información, para los activos definidos como prioridad en el análisis de riesgo realizado, tomando como base la norma ISO/IEC 27001:2013, para el proceso de backup.

✓ Definir los roles y responsabilidades en la organización, para la definición del subsistema de gestión de la seguridad de la información para el proceso de backup.

✓ Socializar la política de tratamiento de información con el personal de la compañía, que hace parte del proceso de backup.

✓ Definir los controles que se deben implementar en el proceso de backup, teniendo en cuenta la política de tratamiento de información y los análisis de riesgos de seguridad de la información en el mencionado proceso.

IV. MARCO TEORICO

Las empresas existen para crear valor para sus propietarios o accionistas, en consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de gobierno, lo que significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo. [1]

La empresa de transportes Tescotur Ltda, dentro de sus metas corporativas tiene como prioridad la satisfacción del cliente, por ende, es necesario realizar un proceso de certificación en las principales normas de calidad para dar garantía y agregar valor a los servicios prestados, cumpliendo estándares que le permiten atender adecuadamente las solicitudes que demandan sus usuarios.

Como primer paso se generará una política general de gestión de seguridad de la información para la empresa de transportes con el fin de que, desde la alta gerencia hasta la base, se comprometan con la adecuada gestión de seguridad de la información y así poder delimitar la política que se pretende implementar para los backups, esto para asegurar los recursos tanto económicos, humanos y tecnológicos con el fin de llevar a feliz término este proceso.

Se pretende realizar el subsistema de backups tomando como base la norma ISO/IEC 27001:2013, complementando el subproceso con la aplicación de metodología de análisis de riesgos bajo la norma ISO/IEC 27005 ya que está orientada a realizar análisis de riesgos en seguridad de la información.

ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO), la cual especifica los requisitos necesarios para la gestión de la seguridad de la información en cualquier tipo de organización. La publicación más reciente fue realizada en el año 2013, de donde toma su nombre ISO/IEC 27001:2013. Su primera versión fue publicada en el año 2005 y se basó en la norma británica BS 7799-2.

ISO/IEC 27001 permite que una empresa sea certificada, lo que indica que una entidad de certificación independiente confirma que la seguridad de la información implementada cumple con los lineamientos indicados en la norma.

Por otro lado, la norma ISO/IEC 27005 entrega directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO / IEC 27001 y fue diseñada para la ejecución satisfactoria de seguridad de la información basado en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la norma ISO / IEC 27001 e ISO / IEC 27002 son necesarios para comprender completamente la norma ISO / IEC 27005. ISO / IEC 27005: 2009, también puede usarse en cualquier tipo de organización tales como empresas comerciales, empresas estatales y organizaciones sin fines de lucro, que deseen gestionar los riesgos que puedan comprometer la seguridad de la información de la organización.

Para el tratamiento del riesgo el proyecto se enfocará en la norma ISO/IEC 27005 la cual ofrece principios y directrices genéricas sobre gestión de riesgos, ya que es la referencia mundial en sistemas de gestión de riesgos, y se eligió teniendo en cuenta que la organización se encuentra en un proceso de recertificación en ISO 9001, siendo necesario ajustar el tratamiento del riesgo con una norma general, sin embargo se tomarán los catálogos de amenazas, vulnerabilidades y valoración de activos contenidos en esta norma para afianzar

el proceso de evaluación del riesgo en las TI, enfocados a la gestión de backups.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA (Plan Do Check Act por sus siglas en inglés), tradicional en los sistemas de gestión de la calidad.

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI. [4]

Fig.1 Ciclo Demming (PDCA) basado en la norma ISO 27000

El hecho de enfocar un SGSI según la norma ISO/IEC 27001 puede aportar las siguientes ventajas a la organización:

- Gestionar un SGSI en una organización, sin importar su tamaño o carácter público o privado.
- Reduce el riesgo de que se produzcan pérdidas de información, con o sin intensión.
- Provee estándares para realizar una revisión periódica, que permite la retroalimentación y mejoramiento continuo.
- Establece una metodología clara, entendible para la alta gerencia, permitiendo la toma de decisiones cuando se requiera.
- Contar con el sistema de gestión, obliga a la realización de auditorías externas de manera periódica, permitiendo identificar las incidencias que se pueden presentar, fomentando la mejora continua.
- Permite ofrecer una garantía a clientes y socios estratégicos, dado que muestra a la organización como una entidad que se preocupa por la confidencialidad y seguridad de la información.
- Permite la integración con otros sistemas de gestión normalizados con otras normas ISO vigentes.
- Ayuda a la organización en el cumplimiento de normas legales vigentes relacionadas con la información y el manejo de información sensible.
- Mejorar el buen nombre e imagen de la organización, frente a la competencia.

V. METODOLOGIA

En el desarrollo de este proyecto se trabaja como metodología la norma ISO 27005, en cuanto al análisis de riesgo, dado que esta norma sigue los lineamientos de gestión de riesgo entregados en la norma ISO 27001.

Esta norma se basa en el modelo iterativo que se muestra en la Figura2. Proceso de gestión de riesgo en la seguridad de la información, en donde se definen las fases a realizar.

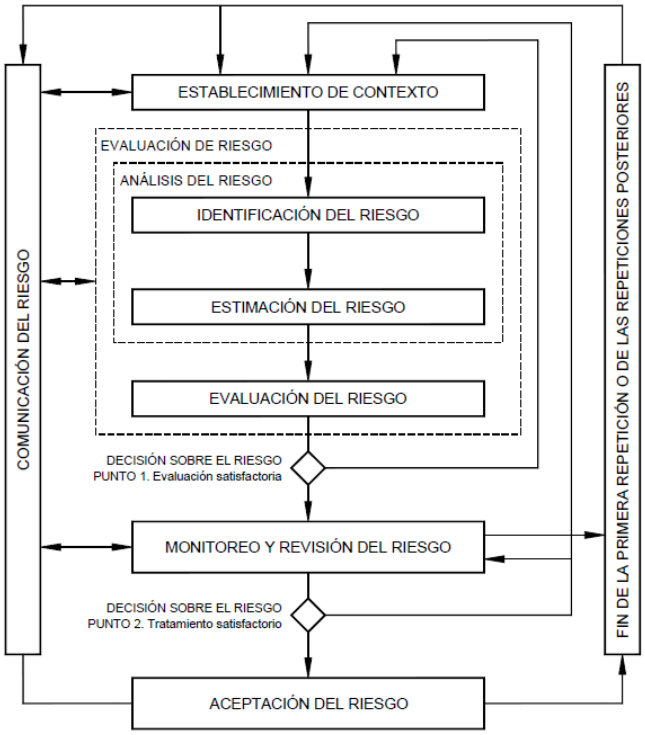


Fig.2 Proceso de gestión de riesgo en la seguridad de la información

De acuerdo a esta norma, en el desarrollo de este proyecto se establece el contexto definiendo los criterios de probabilidad, impacto y la matriz de calor correspondiente; posteriormente se realiza la valoración del riesgo mediante la definición de activos, amenazas y vulnerabilidades, con lo que se obtendrán los niveles de riesgo para cada uno de los activos, los cuales serán evaluados para determinar cuáles de estos riesgos son aceptables y cuáles deben ser tratados; finalmente se realiza el plan de tratamiento.

VI. DESARROLLO DEL PROYECTO

El proyecto se desarrolla teniendo en cuenta las metodologías descritas en el…Capítulo V… de este documento, a continuación, describimos cada una de las etapas realizadas en el proceso.

A. Establecimiento del contexto: Tescotur Ltda es una empresa dedica a la prestación de servicios de transporte especial de pasajeros, cuya información de operación esta almacenada y administrada en un software Web denominado Sistema ERP.

Adicionalmente, cuenta con un software contable SIIGO en el cual se administra la información financiera de la compañía que, de acuerdo a la normatividad vigente en Colombia, debe mantenerse hasta por 5 años y debe permitir la generación de reportes solicitados por entidades gubernamentales tales como impuestos, información exógena, certificaciones de retenciones, entre otros.

Cada uno de los usuarios del área administrativa tienen a su disposición un equipo de cómputo, desde el cual acceden al sistema contable y de operaciones, de acuerdo al cargo asignado en la compañía, además de almacenar la información generada como resultado de las labores realizadas.

Con la información allí almacenada, generan nueva información de reportes, licitaciones, certificaciones, entre otros.

Por otro lado, de manera reciente la compañía ha decidido adquirir un servidor de impresiones, para el control de la papelería generada por sus empleados, con el ánimo de controlar el uso del papel y la tinta.

Con el subsistema de gestión de seguridad para el proceso de backup, se pretende tener respaldo de la información contenida en los sistemas de información anteriormente mencionados, de tal manera que se garantice la confidencialidad, integridad y disponibilidad de la información cuando esta sea requerida.

B. Criterio de evaluación del riesgo: Para valorar los activos dentro de Tescotur LTDA es muy importante usar una escala común o criterio semejante, que permita obtener, a través de un análisis, una valoración correctamente definida que indique la importancia dentro de la empresa.

Para este proyecto, la valoración de los activos se realiza por aproximación cuantitativa para confidencialidad, integridad y disponibilidad, teniendo en cuenta los diferentes factores que conllevan a mantener la información asegurada bajos las consideraciones de:

- Obligaciones legales.
- Intereses comerciales y económicos.
- Información financiera.
- Información de usuario que genere reprocesos por su no disponibilidad.

C. Criterios de Probabilidad: Se solicitó al outsourcing que actualmente presta el servicio de mesa ayuda, la información de los diferentes eventos relacionados con pérdida o modificación de información que se presentan en la compañía, obteniendo el Cuadro I. Eventos de pérdida de información.

CUADRO I
Eventos de pérdida de información

Robo de información
Perdida de histórico financiero
Daño de disco duro
Manipulación no autorizada de la información
Eliminación de archivos de código fuente
Perdida de registros
Des configuración de base de datos
Manipulación no autorizada de la información
Eliminación de archivos

Adicionalmente, se revisaron los reportes del último año, sobre los casos atendidos por la mesa de ayuda, para la definición de la frecuencia con la que ocurren estos eventos y se asignó un valor numérico a las frecuencias establecidas, obteniendo el Cuadro II. Frecuencia con la que se puede dar el evento.

CUADRO II
Frecuencia con la que se puede dar el evento

Valoración	**Niveles de probabilidad**
5	SEMANAL
4	MENSUAL
3	TRIMESTRAL
2	SEMESTRAL
1	ANUAL

D. Criterio de Impacto: Con cada uno de los eventos, se estableció el Cuadro II. Tiempo de suspensión de la operación, la cual indica el impacto que tiene en la compañía la ocurrencia de los eventos, de acuerdo al tiempo de suspensión de las operaciones, que corresponde al tiempo en el que una de las áreas no puede prestar su servicio o un usuario no puede realizar las labores para las cuales fue contratado.

CUADRO III
Tiempo de suspensión de la operación

Valoración	**Tiempo**
5	Más de 4 semanas
4	4 Semanas
3	2 semanas
2	1 Semana
1	Menos de una semana

E. Criterios de aceptación del riesgo: Los criterios de aceptación de riesgo definidos por Tescotur LTDA, indica sobre qué niveles se deben tratar los riesgos.

Los riesgos que se consideran inaceptables están demarcados bajo la matriz con nombre "Alto “y deben ser tratados

inmediatamente bajo los procedimientos establecidos para cada uno de ellos, seguido de estos están demarcados los criterios con un nivel “Medio” y “Bajo” cuyo tratamiento está relacionado al control que corresponda, siempre y cuando mitigue el riesgo con un costo/beneficio acorde a los objetivos del negocio.

CUADRO IV
Matriz de calor nivel de riesgo

Nivel de impacto	**Nivel de Riesgo**				
(5) Más de 4 semanas	5	10	15	20	25
(4) 4 Semanas	4	8	12	16	20
(3)2 semanas	3	6	9	12	15
(2) 1 Semana	2	4	6	8	10
(1) Menos de una semana	1	2	3	4	5
	1 (ANUAL)	2 (SEMESTRAL)	3 (TRIMESTRAL)	4 (MENSUAL)	5 (SEMANAL)
	Probabilidad				

Tratamiento	**Inaceptables**
Medio	Alto
Bajo	

VII. VALORACION DEL RIESGO

A. Identificación de los Activos: De acuerdo al contexto, se define que los activos de información sobre los cuales se realiza el análisis de riesgo, son los relacionados en el Cuadro V. Activos de información.

CUADRO V
Activos de Información

Nombre Activo	**Responsable**	**Ubicación**	**Función**
SISTEMA CONTABLE	OUTSOURCING IT	OF. ADMINISTRATIVAS BOGOTA	Software de administración de información financiera (SIIGO)
SISTEMA DE OPERACIONES (ERP)	OUTSOURCING IT	OF. ADMINISTRATIVAS BOGOTA	Software de administración de información sobre operación de transportes
EQUIPOS USUARIOS	USUARIOS	OF. ADMINISTRATIVAS BOGOTA	Información generada por los usuarios, de acuerdo a las labores que realiza en la compañía
SERVIDOR DE IMPRESIONES	OUTSOURCING IT	OF. ADMINISTRATIVAS BOGOTA	Administración de colas de impresión, e información de uso de suministros de impresión.

B. Identificación de las amenazas: La identificación de las amenazas se realizó teniendo en cuenta el reporte entregado por el outsourcing, de los eventos atendidos relacionados con los activos de información definidos en el numeral anterior.

CUADRO VI
Amenazas

Amenaza	**Origen**	**Tipo**
Usuarios con acceso al sistema	Deliberadas, Accidentales	Personal
Pérdida de suministro de energía	Accidentales	Perdida de los servicios Esenciales
Factores ambientales (Humedad, altas temperaturas)	Ambientales	Ambientales
Personal técnico o de soporte	Deliberadas, Accidentales	Personal
Daños de Hardware	Accidentales	Hardware
Usuarios sin capacitación	Deliberadas, Accidentales	Personal
Espionaje remoto	Deliberadas	Intrusos
Hurto de equipo	Deliberadas	Intrusos
Falla del equipo	Accidentales	Hardware
Mal funcionamiento del equipo	Accidentales	Hardware
Incumplimiento en el mantenimiento del sistema de información	Deliberadas	Software

C. Identificación de las vulnerabilidades y consecuencias: De acuerdo a la definición de las amenazas conocidas, genera el Cuadro VII Vulnerabilidades y consecuencias de cada uno de los activos.

CUADRO VII
Vulnerabilidades y consecuencias

Nombre activo	Amenaza	Vulnerabilidades	Consecuencias
SISTEMA CONTABLE	Usuarios con acceso al sistema - Espionaje remoto - Incumplimiento en el mantenimiento del sistema de información	Facilidad para acceder a los medios de almacenamiento	Perdida de dinero - Incumplimientos con proveedores - Incumplimientos legales
	Usuarios con acceso al sistema -Incumplimiento en el mantenimiento del sistema de información	Facilidad para acceder a los medios de almacenamiento	Incumplimientos Legales
	Pérdida de suministro de energía - Factores ambientales - Personal de soporte técnico - Daños de Hardware -Mal funcionamiento del equipo	Falta de control de hardware	Perdida de dinero - Incumplimientos con proveedores - Incumplimientos legales
	Usuarios con acceso al sistema- Espionaje remoto -Incumplimiento en el mantenimiento del sistema de información	Mala asignación de roles por usuario de TI	Perdida de dinero - Incumplimientos con proveedores - Incumplimientos legales
SISTEMA DE OPERACIONES (ERP)	Personal técnico o de soporte - Espionaje remoto	Facilidad para acceder a los medios de almacenamiento	Retrasos en la prestación del servicio - Disponibilidad del sistema - Perdida de credibilidad
	Personal técnico o de soporte - Espionaje remoto - Usuarios sin capacitación	Mala asignación de roles por usuario de TI	Retrasos en la prestación del servicio - Disponibilidad del sistema - Perdida de credibilidad
	Personal técnico o de soporte - Incumplimiento en el mantenimiento del sistema de información	Mala asignación de roles por usuario de TI	Retrasos en la prestación del servicio - Disponibilidad del sistema - Perdida de credibilidad
	Personal técnico o de soporte - Incumplimiento en el mantenimiento del sistema de información - Espionaje remoto - Usuarios sin capacitación	Mala asignación de roles por usuario de TI	Retrasos en la prestación del servicio - Disponibilidad del sistema - Perdida de credibilidad
	Factores eléctricos - Factores ambientales - Personal de soporte técnico - Daños de Hardware	Falta de control de hardware	Retrasos en la prestación del servicio - Disponibilidad del sistema - Perdida de credibilidad
INFORMACION EQUIPOS USUARIOS	Usuarios sin capacitación - Personal técnico o de soporte	Manipulación por parte del usuario	Incumplimientos Legales - Retrasos en la prestación del Servicio
	Personal técnico o de soporte - Daños de Hardware - Falla del equipo	Falta de control de hardware	Incumplimientos Legales - Retrasos en la prestación del Servicio
	Personal técnico o de soporte - Daños de Hardware - Incumplimiento en el mantenimiento del sistema de información	Acceso a los equipos por usuarios no autorizados - Falta de control de hardware	Incumplimientos Legales - Retrasos en la prestación del Servicio - Perdida de credibilidad
SERVIDOR DE IMPRESIONES	Usuarios sin capacitación - Personal técnico o de soporte	Mala asignación de roles por usuario de TI	Perdida de reportes de costos de impresión
	Factores eléctricos - Factores ambientales - Personal de soporte técnico - Daños de Hardware	Falta de control de hardware	Perdida de reportes de costos de impresión

Después de haber realizado el análisis de riesgos, se van a dar tratamiento a aquellos que se encuentran en los niveles de riesgos inaceptables de la matriz mencionada en el cuadro IV Matriz de calor nivel de riesgo.

VIII. TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

El principal objetivo de este tratamiento, es reducir al mínimo los riesgos inaceptables dentro de Tescotur LTDA, para esto, se tienen cuatro opciones de implementación que se

deberán aplicar de acuerdo al nivel de prioridad y su calificación para cada uno de los riesgos de los activos.

La norma ISO 27005 maneja 4 opciones de tratamiento del riesgo, las cuales se definen de la siguiente forma:

Reducción del Riesgo: Esta opción nos permite ante la selección de controles adecuados la reducción del riesgo, logrando así que este pueda ser evaluado nuevamente y llevarlo a un nivel aceptable.

Retención del Riesgo: Esta opción está encaminada a tomar una decisión severa donde se definirá si el riesgo es aceptado y este satisface tanto las políticas de seguridad como los criterios de la organización.

Evitación del Riesgo: Esta opción de tratamiento pretende retirar una acción o actividad que se origina a partir de un riesgo dentro de un activo, esto cuando el costo de implementación sobrepasa el beneficio al cual se está aplicando.

Trasferencia del Riesgo: Esta opción busca tener un respaldo y compartir un riesgo con otro grupo o un tercero, de esta forma, este riesgo puede ser minimizado en conjunto al compartirlo con otros.

Con base en lo anterior, se establecieron tres niveles de riesgos y su rango de calificación.

CUADRO VIII
Rango calificación de riesgo

Nivel de riesgo	Calificación
ALTO	MAS DE 10
MEDIO	ENTRE 5 Y 9
BAJO	MENOR A 5

Dado el nivel de riesgo obtenido en la evaluación para cada uno de los activos, en el Cuadro IX. Rango calificación Evaluación de Activos – Nivel de riesgo, se evidencian los riesgos inaceptables los cuales tendrán un plan de tratamiento para su mitigación.

CUADRO IX
Rango calificación Evaluación de Activos – Nivel de riesgo

Nombre activo	Descripción del riesgo	Nivel de riesgo	Criterio de aceptación
INFORMACION EQUIPOS USUARIOS	Manipulación no autorizada de la información	16	Alto - Inaceptable
SISTEMA DE OPERACIONES	Desconfiguración de base de datos	12	Alto - Inaceptable
(ERP)	Manipulación no autorizada de la informacion	12	Alto - Inaceptable
INFORMACION EQUIPOS USUARIOS	Eliminación de archivos	12	Alto - Inaceptable
SISTEMA DE OPERACIONES (ERP)	Perdida de registros	10	Alto - Inaceptable

IX. DECLARACION DE APLICABILIDAD

A través de esta etapa se evalúa el cumplimento que tiene Tescotur LTDA en cuanto a la seguridad de la información que contemplan los controles bajo la norma ISO/IEC 27001, dentro del proceso de desarrollo de este proyecto, se han implementado algunas mejoras en los controles, lo que lleva a identificar donde se tienen oportunidades de mejora y donde se necesita un mayor grado de concentración con las falencias encontradas.

Para la realización de la evaluación de los controles que están en el Anexo A de la norma ISO/IEC 27001 se debe tener en cuenta el Cuadro X. Convenciones del nivel de cumplimiento de controles.

CUADRO X
Convenciones del nivel de cumplimiento de controles.

Nombre	Descripción
Implementado	Control completamente implementado o requiere de mínimas reformas para que se cumpla.
No Implementado	Este control no se encuentra implementado, se debe realizar todo el proceso de implementación.
No Aplica	Este control no aplica a la compañía.

Una vez detallados cada uno de los controles de la norma ISO/IEC 27001 y su estado actual de implementación, se obtienen los resultados indicados en el Cuadro XI. Indicador de estado de controles.

CUADRO XI
Indicador de estado de controles

Nivel	Cantidad Controles
Implementado	39
No Implementado	18
No Aplica	57

Se puede apreciar que, de los 114 controles, se encontraron 39 controles Implementados en Tescotur LTDA, así mismo 57 controles que no aplican a la organización para el proceso de backups y 18 controles que no están implementados.

La distribución de estos controles dada en porcentajes se muestra en la Figura 3. Distribución de controles por estado:

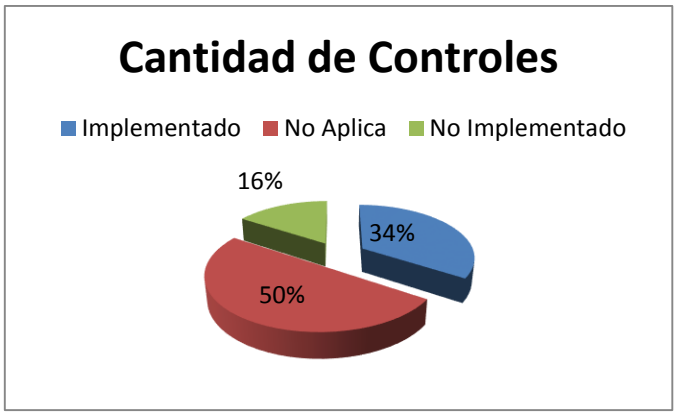


Fig.3 Distribución de controles por estado

X. PLAN DE TRATAMIENTO DE RIESGOS

El plan de tratamiento de riesgos tiene como fin dar el tratamiento a los riesgos inaceptables, de acuerdo a los niveles de aceptación determinados por la empresa.

El costo - beneficio de los controles seleccionados: se realiza teniendo en cuenta el costo de la implantación del control, el tiempo de implantación y el nivel de impacto al omitir el control, en cuanto a tiempo de suspensión de la operación.

Para realizar la evaluación de los criterios mencionados, se aplicaron las métricas indicadas en el Cuadro XI Costo de implantación de control, Cuadro XII Tiempo de implantación y Cuadro XIII Tiempo de suspensión de operación.

Cuadro XI
Costo de implantación de control

Valoración	Numero de SMMLV
1	Hasta 1 SMMLV
2	Mayor a 1 SMMLV y Hasta 3 SMMLV
3	Mayor a 3 SMMLV y Hasta 7 SMMLV
4	Mayor a 7 SMMLV

Cuadro XII
Tiempo de implantación

Valoración	Tiempo
1	Hasta 1 Semana
2	Mayor a 1 semana y hasta 4 semanas
3	Mayor a 4 Semanas y hasta 8 Semanas
4	Mayor a 8 Semanas

Cuadro XIII
Tiempo de suspensión de operación

Valoración	Tiempo
1	Menos de una semana
2	1 Semana
3	4 Semanas
4	Más de 4 semanas

Teniendo la valoración de los tres criterios, se calcula un promedio de ((costo de implantación + tiempo de implantación + tiempo de suspensión) /3), el cual indica el costo beneficio, que se evalúa de acuerdo a la métrica indicada en el Cuadro XIV. Costo – Beneficio.

Cuadro XIV
Costo – Beneficio

Valoración	Costo - Beneficio
1	Es superior respecto a los demás controles.
2	Es mayor respecto a los demás controles
3	Es moderado respecto a los demás controles
4	Es menor respecto a los demás controles

A continuación, se presenta la guía de implantación de los controles seleccionados, de acuerdo a las indicaciones dadas por la norma ISO 27001:2013 en su anexo A y que están asociados a mitigar los riesgos de los activos dentro de la matriz de los niveles inaceptables:

A.5.1.1 Políticas para la seguridad de la información. Este documento contiene los objetivos, alcances, normas, cumplimiento de requisitos legales, de educación, formación y concientización de seguridad de la información relacionada con activos definidos en este proyecto; además de la gestión de continuidad y consecuencias del incumplimiento de la política, complementado con la intensión de la dirección en apoyo a las metas de seguridad establecidas.

A.6.1.1 Roles y responsabilidades para la seguridad de la información. Definición de los roles y responsabilidades, de acuerdo a la política de seguridad, asegurando el cumplimiento de los objetivos de seguridad.

A.7.2.1 Responsabilidades de la dirección. Compromiso de la dirección en la exigencia a empleados y contratistas, del cumplimiento de la seguridad de la información de acuerdo a lo establecido en la política.

A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. Realización de jornadas educativas e informativas, cuando ingresen empleados o contratistas nuevos y con frecuencia semestral para empleados y contratistas antiguos, permitiendo que se mantengan informados de las políticas establecidas, sus roles y responsabilidades y el manejo de incidentes.

A.8.1.2 Propiedad de los activos. Definición de los responsables de cada uno de los activos identificados.

A.8.1.3 Uso aceptable de los activos. Definición de los lineamientos de uso de los activos, de acuerdo a la política de seguridad implementada.

A.9.1.1 Política de control de acceso. Definir la política de control de acceso de acuerdo a la clasificación de la información y a la política de seguridad establecida. Esta política de control de acceso debe tener reglas claras de acuerdo a los roles y responsabilidades.

A.9.2.1 Registro y cancelación del registro de usuarios. Definición del proceso de creación y cancelación de usuarios, con acceso a los sistemas de información y backup, para contratistas y empleados de acuerdo a los roles y responsabilidades establecidos.

A.9.2.2 Suministro de acceso de usuarios. Definición de procedimiento para la asignación de acceso de usuarios a los sistemas y servicios, teniendo en cuenta los roles y responsabilidades establecidos.

A.9.2.3 Gestión de derechos de acceso privilegiado. Definición de procedimiento para la asignación de acceso privilegiado, para los usuarios registrados, de acuerdo a los roles y responsabilidades establecidos.

A.9.2.5 Revisión de los derechos de acceso de usuarios. Revisión semestral de los derechos de acceso asignados a los usuarios del sistema, realizada por los propietarios de los activos, de acuerdo a la política establecida.

A.9.2.6 Retiro o ajuste de los derechos de acceso. Procedimiento que establezca los lineamientos necesarios, para realizar el retiro de usuarios o ajuste de los derechos de acceso, una vez se termina la relación por acuerdo o contrato, entre la empresa y empleados o contratistas.

A.9.4.1 Restricción de acceso a la información. Generar las restricciones necesarias para el acceso a la información, de acuerdo a la política de control de acceso establecida por la compañía.

A.12.3.1 Respaldo de la información. Se debe realizar copias de seguridad, de acuerdo a la frecuencia establecida en la política de copias de respaldo, realizando las pruebas de verificación necesarias.

A.12.4.1 Registro de eventos. Realizar el registro de los eventos relacionados con el proceso de backups, mediante logs del sistema operativo y bitácora realizada por el responsable.

A.13.1.1 Controles de redes. Realizar verificación de transferencia de información en la red local trimestralmente, y aplicar las correcciones necesarias cuando sea notificada alguna falla. Aplicar restricciones de acceso a información de dispositivos de almacenamiento de información, de acuerdo a los roles y responsabilidades definidos.

XI. OBJETIVOS DE SEGURIDAD DE LA INFORMACION

Como estrategia para proteger los activos de información de la empresa Tescotur LTDA, es indispensable definir las acciones y responsables de los controles establecidos en la norma ISO/IEC 27001, que permitan el cumplimiento de los siguientes objetivos de seguridad:

- Crear conciencia de la importancia de la seguridad de la información en todos los miembros de la organización, de tal manera que se comprometan en el cumplimiento de las normas establecidas en la política de seguridad.

- Asegurar que la alta gerencia se comprometa en el cumplimiento de la normatividad establecida, exigiendo a todos los miembros de la organización la implementación de los procedimientos establecidos y el buen uso de la información, de acuerdo a los roles y responsabilidades asignados.

- Garantizar que los respaldos de información se realicen bajo los procedimientos establecidos.

- Retroalimentar de manera efectiva el SGSI establecido, permitiendo su mejora continúa mediante la identificación de vulnerabilidades y aplicación de controles que permitan su mitigación.

Las acciones definidas tienen la aprobación de la dirección y cuentan con el compromiso de planeación para su seguimiento y cambio a futuro.

XII. CONCLUSIONES

- ✓ Para este proyecto se seleccionó la norma ISO/IEC 27005 como metodología para la realización del análisis de riesgos, como complemento de la norma ISO/IEC 27001, porque explica de manera clara el proceso necesario para la realización de un análisis de riesgos detallado, como se requiere en este caso.

- ✓ Los controles seleccionados fueron tomados del anexo A de la norma ISO/IEC 27001, dado que entrega controles estandarizados y clasificados, que permite identificar de manera clara y fácil los riesgos que pueden ser reducidos con su aplicación.

- ✓ Durante el levantamiento de información para la realización del análisis de riesgos, se pudo identificar que en la compañía no estaban plenamente definidos los roles y responsabilidades de empleados y contratistas; sin embargo, gracias a este análisis la compañía logró identificarlos e implementarlos antes de completar el proceso del análisis de riesgos.

- ✓ Con la realización del análisis de riesgo, encontramos que la empresa ha venido implementando controles de

seguridad, sin tener conocimiento previo sobre los estándares o metodologías propias de la seguridad informáticas. Estos controles se han aplicado basados únicamente en las necesidades tecnológicas de la organización, y en su mayoría sugeridas por el outsourcing de tecnología actualmente contratado.

- ✓ Con la realización de este proyecto, los directivos de la empresa participaron activamente y dieron a conocer su interés en continuar con el proceso para llegar a la implementación del sistema de seguridad propuesto, además de identificar otros procesos en los cuales se requiere el diseño e implementación de un SGSI siguiendo los lineamientos de la norma ISO/IEC27001.

- ✓ Con la realización del análisis de riesgos, los directivos se dieron cuenta de los fallos de seguridad con los cuales han venido trabajando, incluso que no son propios del subproceso de backup, y entendieron que la implementación de un SGSI en la organización es realmente una inversión, que, aunque no generará dinero, si permitirá preservar su prestigio y buen nombre, además de ahorrar en gastos en los que puedan incurrir en el caso de explotarse una vulnerabilidad.

- ✓ Con el desarrollo el proyecto también se evidencio, que las principales vulnerabilidades vienen de los empleados de la organización. Con la realización de las jornadas de concientización, se logró que los empleados y directivos vieran la importancia de una buena administración de la información.

- ✓ A través de la realización de este proyecto en la organización, los empleados que participaron en el levantamiento de información, lograron darse cuenta que muchos de los fallos de seguridad que se pueden presentar en una organización, tienen origen en las acciones cotidianas de cualquier persona, tales como prestar contraseñas por “ayudar” a un compañero de trabajo, o compartir el formato de un documento que sin darse cuenta contiene información de la cual solo él es responsable.

REFERENCIAS

[1] INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma técnica Colombiana para la presentación de tesis, trabajos de grado, y otros trabajos de investigación. Bogotá D.C., INCONTEC, 2008. NTC 1486.

[2] INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma técnica Colombiana para referencias documentales para fuentes de información electrónica. Bogotá D.C., INCONTEC, 1998. NTC 4490.

[3] INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma técnica Colombiana para referencias bibliográficas, contenidos, forma y estructura. Bogotá D.C., INCONTEC, 2008. NTC 5613.

[4] [1] COBIT® 5 ISACA - Derechos de autor © 2012 ISACA. Todos los derechos reservados. Para pautas de uso, ver www.isaca.org/COBITuse.